国内外互联网研究系列丛书

美国国家网络安全战略研究

程　工　孙小宁　张　丽　石　瑾　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

随着各国在互联网安全领域的交流与对话日益深入，制定网络安全的国家安全战略，对于有效调动协调各方力量，更好地保护国家利益，显得至关重要。作为互联网大国，美国拥有最先进的互联网技术，同时也面临着来自网络的严峻威胁与挑战，因此一直以来美国对于互联网安全给予了高度重视。本书通过重点研究美国近年来的网络安全战略走向，分析美国网络安全战略的制定与不断演进过程中的有益经验与做法，希望为我国制定国家层面的网络安全战略提供借鉴和参考。

本书理论与实际相结合，对于各级党政机关和企业开展网络舆情的监测和分析工作，充分发挥其在信息决策中的作用，具有重要的参考意义。也可供网络舆情研究领域的各类学术机构的工作人员和学生阅读参考。

图书在版编目（CIP）数据

美国国家网络安全战略研究 / 程工等编著. —北京：电子工业出版社，2015.11
（国内外互联网研究系列丛书）
ISBN 978-7-121-27472-5

Ⅰ. ①美… Ⅱ. ①程… Ⅲ. ①计算机网络－国家安全－国家战略－研究－美国 Ⅳ. ①D771.235 ②TP393.08

中国版本图书馆 CIP 数据核字（2015）第 258099 号

责任编辑：徐蔷薇　　特约编辑：王　纲
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　　印张：16.5　字数：412 千字
版　　次：2015 年 11 月第 1 版
印　　次：2015 年 11 月第 1 次印刷
定　　价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

2015 年 7 月 6 日，《网络安全法》（草案）经十二届全国人大常委会第十五次会议初次审议后，正式全文发布并向全社会公开征求意见。这是我国网络安全工作的一件大事，彰显了国家对于网络安全问题的高度重视，同时也标志着网络安全被提升到国家安全与发展层面，为建设“网络强国”的战略部署提供了法律支撑和保障。事实上，各国政府对于网络攻击的威胁，对于网络关键基础设施的保护，对于统筹国家和民间力量，从宏观和微观两个层面建设本国的网络安全体系框架，早已有了共识。至少有 41 个国家颁布了各种形式的网络空间安全的国家战略，旨在加强本国网络安全方面的攻防能力。而其中，作为世界上互联网最发达的国家，同时也是走在网络安全技术最前沿的国家，美国对于网络安全的重视程度，也是各国之中最为突出的。从 20 世纪 80 年代起，至 2015 年 6 月底，美国以战略、计划、总统令等多种形式，先后颁布了 40 多份与网络安全相关的文件，构成了一个较为完备的网络安全战略体系。本书重点选取了克林顿、布什和奥巴马三位最近的美国总统执政期间推出的相关战略文件，对其战略的演变脉络以及相关举措进行了梳理和分析。

本书与 2014 年出版的《国外网络与信息安全战略研究》是姊妹篇，所有内容都围绕美国的网络安全战略体系，分为三章：第一章为美国网络安全战略分析，第二章为美国网络安全战略概要，第三章为美国网络安全战略译文。希望本书能够为关注网络安全战略问题的读者提供借鉴和参考。

编　者

2015 年 7 月

目　　录

第一章　美国网络安全战略分析

美国政府历年重要网络与信息安全文件概述

作为世界上互联网最发达的国家之一，美国对互联网的应用程度和依赖程度远高于大多数国家，因而面临更大的网络和信息安全威胁。20 世纪 80 年代以来，美国政府对网络安全的重视程度不断提升，并视之为国家安全的重要组成部分。截至 2015 年，美国先后颁布了 40 多份与网络安全有关的文件，形式包括战略、计划、行政令、总统令等。本书重点研究克林顿、布什和奥巴马三届美国总统执政期间所推出的与网络和信息安全相关的战略文件。

一、克林顿政府时代（1992—2001 年）

美国的网络安全政策产生于克林顿政府时期保护关键基础设施的行动。克林顿总统在 1996 年签发了第 13010 号行政命令，创立了总统关键基础设施保护委员会，并强调了网络攻击对国家的经济和国防安全的威胁。在该委员会的建议下，克林顿总统在 1998 年 5 月签发了第 63 号总统决策令。

（一）第 63 号总统决策令：《克林顿政府对关键基础设施保护的政策》（Presidential Decision Directive 63：The Clinton Administration’s Policy on Critical Infrastructure Protection）

1998 年 5 月 22 日，克林顿政府发布了第 63 号总统决策令（PDD63）：《克林顿政府对关键基础设施保护的政策》，第一次就美国信息安全的概念、意义、长期与短期目标等做出了明确的说明，并针对下一步的行动做了指示。克林顿政府在 PDD63 中指出，“我们的经济越来越依靠那些相互依赖的、由计算机和网络支持的基础设施，对我们的基础设施和信息系统的非常规攻击有可能使我们的军事和经济力量遭到巨大伤害。”

PDD63 提出，最迟不晚于 2000 年，美国应当实现初步的信息保障能力。PDD63 要求从总统令发布之日起，五年后美国将获得并保持对国家的关键基础设施进行保护的能力，以防止可能严重危害到下述职能的有预谋的行为：联邦政府履行其重要的国家安全责任并确保公众健康和安全；州和地方政府维持有序运转，提供最起码的重要公共服务；民营部门确保经济有序运行以及重要电信、能源、金融和运输服务的正常提供。这些关键职能遭到的任何破坏或操纵必须控制在短时、低频、可控、地域上可隔离且对美国的利益损害最小的规模。

（二）《信息系统保护国家计划（V1.0）》（National Plan for Information Systems Protection Version 1.0）

2000 年 1 月 5 日，克林顿政府发布了《信息系统保护国家计划（V1.0）》，提出了美国政府在 21 世纪之初若干年的网络空间安全发展规划。克林顿表示，“信息系统保护国家计划是一系列更为复杂的工作的第一步。随着我们对正在出现的威胁和脆弱性的认识不断深入，我们的计算机保护计划将持续发展和更新。它向我们展示了一个综合的方案，为我们的经济、国家安全、公共健康和安全中的关键部门提供了保护措施。为成功实施这个计划，政府和私人业主必须齐心协力，建立一种前所未有的合作关系。只有举国上下团结应战，我们才能达到我们的目标。我们不能指望只依赖政府法令来实现我们的目标，每个部门必须自己决定保护其关键系统所必需的方法、步骤和标准。作为合作关系中的一方，联邦政府随时准备提供帮助。”

（三）《全球时代的国家安全战略》（A National Security Strategy For A Global Age）

2000 年 12 月 1 日，克林顿总统签署了《全球时代的国家安全战略》。签署该文件是美国国家信息与网络安全政策的重大事件。文件将信息安全与网络安全列入国家安全战略，成为国家安全战略的重要组成部分。这标志着网络安全正式进入了国家安全战略框架，并具有了独立地位。

二、布什政府时代（2001—2009 年）

布什总统上台不久，美国便发生了举世瞩目的“9·11”事件，布什政府深刻认识到反恐必须切实加强对国家关键基础设施与资产的保护。因此，布什执政期间对关键基础设施保护的重视程度达到了空前的高度，出台了一系列相关战略文件。此外，分别于 2003 年和 2008 年出台的两份重要文件：《确保网络空间安全的国家战略》和《国家网络安全综合计划》（CNCI），强调了发展保卫国家网络安全的能力。

（一）第 13231 号行政令：《信息时代的关键基础设施保护》（Executive Order 13231：Critical Infrastructure Protection in the Information Age）

2001 年 10 月 16 日，布什政府意识到了“9·11”事件之后信息安全的严峻性，发布了第 13231 号行政令：《信息时代的关键基础设施保护》，宣布成立“总统关键基础设施保护委员会”（PCIPB），代表政府全面负责国家的网络空间安全工作。委员会成立以后，为制定布什政府的国家网络空间安全战略，2002 年 3 月 20 日向美国民众公布了国家战略中可能会涉及的 53 个重点问题并广泛听取了国民的意见和建议。2002 年 9 月 18 日，“9·11”事件一周年纪念日之后，在整理国民对 53 个问题的反馈意见的基础上，发布了《确保网络空间安全的国家战略》（草案）。

（二）《确保网络空间安全的国家战略》（The National Strategy to Secure Cyberspace）

2003 年 2 月 14 日，美国公布了《确保网络空间安全的国家战略》（正式版）。该战略是

布什政府对《美国国土安全的国家战略》（2002 年 7 月公布）的补充，并以《保护至关重要的基础设施和关键资产的国家战略》（2003 年 2 月 14 日公布）作为其补充文件。该战略明确界定了关键基础设施，是指“那些维持经济和政府最低限度的运作所需要的物理和网络系统，包括信息和通信系统、能源、银行与金融、交通运输、水利系统、应急服务、公共安全等部门以及保证联邦、州和地方政府连续运作的领导机构”。

该战略确定了在网络安全方面的三项总体战略目标和五项具体的优先目标。发生网络攻击时，使损害程度最小化、恢复时间最短化。五项优先目标如下。

（1）建立国家网络安全响应系统。

（2）建立一个减少网络安全威胁和脆弱性的国家项目。

（3）建立一个网络安全预警和培训的国家项目。

（4）确保政府各部门的网络安全。

（5）国家安全与国际网络安全合作。

（三）《关键基础设施和重要资产物理保护国家战略》（The National Stategy for The Physical Protection of Critical Infrastructures and Key Assets）

2003 年 2 月 14 日，美国发布了《关键基础设施和重要资产物理保护国家战略》，标志着美国从国家安全的高度全面推行关键基础设施与资产保护计划。该战略将美国的关键基础设施分为 11 项，包括：农业与食品、水、公共卫生、应急服务、国防工业基地、通信、能源、交通运输、金融、化学工业与有害物质、邮政与货运。关键资产则包括核电站、水坝、有害物质存储设备，以及代表国家形象的肖像、纪念馆、政府与商务中心等。

（四）《网络空间安全：迫在眉睫的危机》（Cyber Security: A Crisis of Prioritization）

2005 年 4 月 14 日，美国政府公布了美国总统 IT 咨询委员会 2 月 14 日向总统布什提交的《网络空间安全：迫在眉睫的危机》紧急报告，该报告对美国 2003 年的信息安全战略提出了不同看法，指出过去十年里美国保护国家信息技术基础建设工作是失败的，短期弥补修复不能解决根本问题。全球信息栅格（GIG）耗资 1000 亿美元，仍然漏洞百出，没有解决安全问题。该报告提出了以下问题和建议。

（1）政府对民间网络空间安全研究的资助不足，建议每年向美国国家科学基金会（NSF）增加 9000 万美元的预算支出；

（2）网络空间安全基础性研究团体规模小，建议用七年时间将团体规模扩大一倍；

（3）安全研究成果的成功转化不够，政府应加强在技术转让方面与企业的合作；

（4）政府部门间协作与监管缺乏是安全对策无重点和无效率的根源，建议成立“重要信息基础设施保护的跨部门工作组”。

（五）《国家网络安全综合计划》（The Comprehensive National Cybersecurity Initiative，CNCI）

2008 年 1 月 8 日，美国总统布什签署发布了第 54 号国家安全总统令暨第 23 号国土安全总统令（NSPD54/HSPD2），要求保护美国的网络安全，防止美国遭受敌对的电子攻击，

并能对敌方展开在线攻击。

在布什签署该项总统令后，美国有关部门制定了《国家网络安全综合计划》（CNCI）。该计划的预算至今未公布，据《纽约时报》估计有 400 亿美元，而《华盛顿邮报》声称是数十亿美元。由于是密令，其一直对外保密。2010 年 3 月 20 日，经多方呼吁，美国总统奥巴马高调宣布解密其部分内容，旨在提高透明度以争取民心。部分解密的内容显示，CNCI 有三个重要目标。

（1）通过在联邦政府（最终将在州、地方和部族政府以及民营领域合作者）内部创建和加强对网络漏洞、威胁和事件的共享态势感知能力和对减少当前漏洞和防止入侵的快速反应能力，进而建立一个防御前线以抵御当前面临的迫切威胁。

（2）通过加强美国的反情报能力和增进关键信息技术供应链的安全，进而实现应对全方位威胁的防御能力。

（3）通过扩大网络教育、全面协调和重新定位联邦政府内的研发工作、致力于明确和制定相关战略以阻止敌对和恶意的网络空间行动等措施，进而巩固未来的网络空间环境安全。

（六）《提交第 44 届总统的保护网络空间安全的报告》（Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency）

2008 年 12 月，布什政府成立的“第 44 届总统网络空间安全委员会”经过一年半的工作，形成了《提交第 44 届总统的保护网络空间安全的报告》。随着任期将满，第 43 届美国总统布什希望下一届总统能够解决网络信息安全问题。报告提出网络安全是美国在竞争更加激烈的新国际环境中面临的最大安全挑战之一。报告认为，过去 20 年来，美国一直在努力设计一种战略来应对这些新型威胁并保护自身利益，但始终都不算成功。无效的网络安全以及信息基础设施在激烈竞争中受到攻击，削弱了美国的力量，使国家处于风险之中。该报告建议，在布什时期的网络安全战略基础之上建立一个包括外交、情报、军事、经济的综合性网络安全战略。

报告提出了 12 项、25 条建议，分别从制定战略、设立部门、制定法律法规、身份管理、技术研发等方面进行了阐述。报告指出，网络不仅是一种企业资产，还应作为一种武装系统加以保护，如同国家其他的关键基础设施那样受到保护。针对当前和未来可能的网络攻击，报告重点提出了“设计、运行和保护网络”，确保联合作战的需求。

三、奥巴马政府时代（2009 年至今）

奥巴马在竞选期间就一直强调网络安全对美国的重要性。2009 年 2 月，他在就职后不久即要求对美国的网络安全状况展开为期 60 天的全面评估，检查联邦政府部门保护机密信息和数据的措施。此后，奥巴马政府将制定网络空间战略列为重中之重，先后出台了《网络空间可信身份国家战略》、《网络空间国际战略》、《网络空间行动战略》、《国土安全相关实体网络安全战略》、《网络安全框架》等一系列重要战略文件，构建了一个包含网络安全、网络经济、网络监控、网络自由、网络威慑等在内的全方位战略体系，从战略层面确立美国在网络空间的主导地位，帮助美国实现制网权。

（一）《国家网络安全战略：需要进行的关键改进》（National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture）

2009 年 3 月 10 日，美国联邦审计署发布了《国家网络安全战略：需要进行的关键改进》报告，对需要进一步加强的网络安全关键领域和改进美国国家网络安全战略提出了建议。报告要求采取积极措施，进一步加强五个领域的网络安全，即支持网络分析和预警能力，完成网络安全实践提出的行动，增强基础设施控制系统的网络安全性，加强国土安全部对网络攻击的恢复能力，解决网络犯罪问题。

（二）《网络空间政策评估：保障可信和强健的信息和通信基础设施》（Cyberspace Policy Review：Assuring a Trusted and Resilient Information and Communications Infrastructure）

2009 年 5 月 29 日，奥巴马总统公布了由安全部门官员起草的题为《网络空间政策评估：保障可信和强健的信息和通信基础设施》的报告。报告认为美国的数字基础设施主要建立在互联网基础上，目前并不安全，现状“不可接受”，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。报告共 76 页，正文包括 6 章，分别如下。

（1）加强顶层领导。通过以下事项来加强对网络空间安全的领导：设立总统网络空间安全政策官及支撑机构，审查法律和政策，加强联邦对网络空间安全的领导。

（2）建立数字国家。提升公众的网络安全意识；加强网络安全教育，扩大联邦信息技术队伍，使网络安全成为各级政府领导人的一种责任。

（3）共担网络安全责任。改进民营部门和政府的合作关系，评估公私合作中存在的潜在障碍，与国际社会有效合作。

（4）建立有效的信息共享和应急响应机制。建立事件响应框架，加强事件响应方面的信息共享，提高所有基础设施的安全性。

（5）鼓励创新。通过创新来解决网络空间安全问题；制定全面、协调并面向新一代技术的研发框架，建立国家的身份管理战略；将全球化政策与供应链安全综合考虑；保持国家安全暨应急战备能力。

（6）行动计划。提出了近期行动计划 10 项和中期行动计划 14 项。

（三）《网络空间可信身份国家战略——增强在线选择、效率、安全与隐私保护》（National Strategy for Trusted Identities in Cyberspace——Enhancing Online Choice, Efficiency, Security and Privacy, NSTIC）

2011 年 4 月 15 日，美国白宫发布了《网络空间可信身份国家战略——增强在线选择、效率、安全与隐私保护》（NSTIC），旨在通过政府和企业的共同努力，建立一个以用户为中心的身份生态系统，促使个人和组织遵循协商一致的标准和流程来鉴别和认证数字身份，从而实现相互信任。计划用 10 年左右的时间，构建一个网络身份生态体系，推动个人和组织在网络上使用安全、高效、易用的身份解决方案。为此，美国成立了专门的主管办公室（NPO），负责协调政府和私人部门的活动，并牵头制定实施路线图。NSTIC 将是美国信息高速公路建设后，又一项涉及全球的巨大信息技术工程，美国政府希望借此再次引领世界经济新潮流，

占领未来全球经济的制高点。

（四）《网络空间国际战略——互连世界的繁荣、安全与开放》（International Strategy for Cyberspace——Prosperity, Security and Openness in a Networked World）

2011 年 5 月 16 日，美国联邦政府六大部门——白宫、国务院、司法部、商务部、国土安全局和国防部共同宣布了《网络空间国际战略——互连世界的繁荣、安全与开放》。奥巴马总统在前言当中指出，这是美国第一次针对网络空间设定全盘计划，并且结合政府部门与民间，以及国际盟友来共同实施。战略宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为实现这一构想勾勒出了政策路线图，内容涵盖经济、国防、执法和外交等多个领域，“基本概括了美国所追求的目标”。

该战略列出了七个政策重点：通过制定国际标准、鼓励创新和开放市场，加强知识产权保护；确保网络的安全、可靠和韧性；深化执法合作并积极推出国际规则；强化“网军”以应对 21 世纪的安全挑战；建立有效且多方参与的国际互联网治理架构；展开“网络援外”；保障互联网自由。战略中还提出了网络空间十大“基本原则”，即维护基本自由、尊重知识产权、重视隐私、打击犯罪、维护自卫权、确保网络全球互通、确保网络稳定、确保人人能上网、多方参与的互联网治理，以及给予网络安全应有的重视。

（五）《网络空间行动战略》（Department of Defense Strategy for Operating in Cyberspace）

2011 年 7 月 14 日，美国国防部发布了首份《网络空间行动战略》，以加强美军及重要基础设施的网络安全保护。根据美国国防部网站公开的部分文件内容，该战略包括五大支柱。

（1）将网络空间作为与陆、海、空、外太空并列的“行动领域”，国防部以此为基础进行组织、培训和装备，以应对网络空间存在的复杂挑战和巨大机遇。

（2）变被动防御为主动防御，从而更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为。

（3）加强国防部与国土安全部等其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强重要基础设施的网络安全防护。

（4）加强与美国的盟友及伙伴在网络空间领域的国际合作。

（5）重视高科技人才队伍建设并提升技术创新能力。

（六）《可信网络空间：联邦网络安全研究与发展项目战略计划》（Trustworthy Cyberspace: Strategic Plan for The Federal Cybersecurity Research and Development Program）

2011 年 12 月 6 日，美国白宫发布了路线图，公布了网络安全的研究与发展重点，以确保美国网络基础设施的安全，并改变人们处理网络安全问题的方式。美国首席技术官安尼什·乔普拉与白宫网络安全负责人霍华德·施密特发表博文称，《可信网络空间：联邦网络安全研究与发展项目战略计划》源于 2009 年年初美国总统奥巴马下令开展的一次为期 60 天的国家网络安全状态评估。该评估报告呼吁政府采取紧急行动，以确保美国计算机网络基础

设施的安全。为响应此号召，美国白宫科学和技术政策办公室制订了该研究与发展计划，旨在帮助美国应对网络安全的挑战，并更有效地保护网络空间的安全。

经过全面评估以及公共与民营部门网络安全专家的论证，该计划确定了保护美国网络基础设施的四个战略重点。

（1）运用 “改变游戏规则（game-changing）”的思维来理解网络安全目前的缺陷根源，并找到解决这些问题的新方法。这方面的研究包括建立更多的“动态目标”，使黑客难以渗透到计算机网络。静态、链式的网络更容易招致攻击，因为黑客有更多的时间来计划并执行攻击。

（2）像所有科学实践一样，为网络安全构建科学基础，诸如法律、假设检验、重复实验设计、数据收集方法与指标标准化、常用术语等。

（3）与研究机构合作，协调和整合相关技术，最大限度地发挥研究影响，确保网络安全的研究方向与研究机构的目标相一致。

（4）缩短网络安全从研究到投入实践阶段的时间。

（七）《实现能源输送系统网络安全路线图》（Roadmap to Achieve Energy Delivery Systems Cybersecurity）

2011 年 9 月 15 日，美国能源部发布了《实现能源输送系统网络安全路线图》，确定了 2020 年前美国能源输送系统网络安全目标，并给出了应对网络攻击的策略。这份路线图向拥有和控制重要能源基础设施的政府部门和民营企业提出了 5 项战略，呼吁它们精诚合作，为美国打造安全可靠和恢复力强的能源输送系统。

路线图要求：公共和私企的利益相关方应当对风险进行评估和监控，这样才能针对不断演进的网络威胁和漏洞做出快速响应。路线图要求能源领域继续改进安全，并确保公共和私有利益相关方的合作顺利进行。路线图还指出了实现这些目标可能遇到的障碍，其中包括：在能源行业里，技能熟练的工程师和工人不足；在能源输送系统安全风险方面的知识有限、理解不到位、评估不足；安全风险环境迅速变化。

（八）《确保未来网络安全的蓝图：国土安全相关实体网络安全战略》（Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise）

2011 年 12 月 12 日，美国国土安全部网站发表了 2011 年网络安全战略报告，题为《确保未来网络安全的蓝图：国土安全相关实体网络安全战略》。该报告在《四年国土安全评估报告》的基础上撰写，意图是呼吁保护对美国至关重要的关键基础设施，并在不久后开发出更强大的信息和通信技术，使政府、企业和个人更安全地使用互联网。

报告列出了两大行动领域：一是保护当前的关键信息基础设施，二是建设未来的网络生态系统。其中，保护关键信息基础设施的四项目标是：降低网络安全风险；快速应对网络安全事件，提高网络恢复能力；共享网络安全信息；增强网络抗压能力。加强网络生态系统建设的四项目标是：提高个人和组织安全使用网络的能力；研发和应用更可信的网络协议、产品、服务、配置和架构；构建合作型网络社区；建立透明的安全流程。

（九）《国家信息共享及保护战略》（National Strategy For Information Sharing and Safeguarding）

2012 年 12 月 19 日，美国白宫发布了《国家信息共享及保护战略》，允许政府部门间共享信息，建立政府机构间数据共享机制。此举有助于增强打击和防御国外黑客攻击及其他犯罪的能力。该战略的主要目标是：推进网络的互联互通和共享服务数据，通过体制改革以及政策技术方案的支持，建立安全机制。战略还强调网络安全保障不能侵犯公民的隐私和权利。

《国家信息共享及保护战略》全面概括地强调了数据共享的重要性。该战略指出，美国的国家安全在很大程度上取决于信息分享的天时、地利、人和。信息共享的管理工作，需要各联邦州政府、各地方、各民营部门以及国外合作伙伴间长期不懈的合作。此外，奥巴马政府将“信息”视为保障国家基础设施安全的重要“国家资产”，同时也强调保护情报和知识产权的重要性。

（十）第 13636 号行政令：《增强关键基础设施网络安全》（Executive Order 13636：Improving Critical Infrastructure Cybersecurity）

2013 年 2 月 12 日，美国总统奥巴马签署了名为《增强关键基础设施网络安全》的第 13636 号行政令，旨在保护国家基础设施免受网络攻击。该行政令的主要内容包括：在国家层面上，美国总统正式认定“信息战”会一直持续下去，是目前显而易见的威胁。政府将与民营部门合作建立“网络安全框架”（Cybersecurity Framework），实现网络攻击与威胁的信息共享，从而降低针对关键基础设施的网络安全风险。

行政令指出，网络安全基本框架将由美国国家标准与技术研究所（NIST）制定。该框架包含一套标准、方法、步骤、流程以及应对网络安全风险的非指定的技术手段。“网络安全框架”的建立有助于将现有的政府项目向民营部门扩展，从而让更多的民营部门的专家在一段时间内为政府服务。行政令中还规定了建立“网络安全框架”的具体时间表，以及“网络安全框架”对隐私状况的影响的评估报告。行政令呼吁政府和机构加强政策协调，实现更广泛的信息共享，但是该行政令并不具有和法律同等的效力，白宫期望能借此引入立法机制。

（十一）《网络安全框架》（Framework for Improving Critical Infrastructure Cybersecurity V1.0）

2014 年 2 月 12 日，美国政府公布了最新《网络安全框架》，用于协助关键基础设施经营者制定网络安全总体方案。该框架是根据一年前发布的第 13636 号行政令《增强关键基础设施网络安全》的要求制定的。该框架由美国企业与政府历时一年共同完成，由隶属于美国商务部的美国国家标准与技术研究所（NIST）发布。框架搜集了全球现有的标准与做法，采用了风险管理的方法，以便于各机构适应“不断变化的网络安全环境，并对变化中的复杂威胁及时做出响应”。企业可以利用该框架制定一个“可信的”网络安全方案。

《网络安全框架》包括三部分内容。

（1）核心。框架核心（Framework Core）描述了企业在确认网络安全风险、保护企业免遭攻击、如有事故发生开展检测、响应，并从可能造成的任何损害中恢复的整个过程中的高级活动。

（2）概况。框架概况（Framework Profiles）用来描述一个企业安全做法的现状。将一个企业的现状与目标相比，可以衡量该企业与其安全项目目标的差距。

（3）实施层级。框架实施层级（Framework Implementation Tiers）描述随着严密性的提升，具体的过程分为四级，从“部分（partial）”（1 级）到“适应（adaptive）”（4 级）。企业可以根据其商业目标、法律以及监管要求和其他限制条件，自行选择最适合的层级。

美国政府官员表示，他们希望该框架能推动改变企业处理网络安全的方式。虽然是否采纳该框架是自愿行为，不过，美国国土安全部已成立关键基础设施网络社区（C3）志愿项目来提升企业对该框架的认识，协助它们管理风险。

（十二）总统行政令：《促进民营部门网络安全信息共享》（Executive Order：Promoting Private Sector Cybersecurity Information Sharing）

2015 年 2 月 12 日，美国总统奥巴马签署了一项旨在提高关键性基础设施网络安全的行政命令，要求美国政府与运营关键性基础设施的合作伙伴加强信息共享，共同建立和发展一个推动网络安全的实践框架。行政命令要求联邦机构“及时”向运营商提供非保密的网络威胁信息。同时，行政命令还扩大了“强化网络安全服务项目”的覆盖范围，国防基础工业之外的关键性基础设施也可以参与该项目，获得近乎同步的信息共享以提高网络安全防御能力。美国国家标准与技术研究所（NIST）将负责提供技术标准和指导，与关键性基础设施行业共同发展网络安全的实践框架。

奥巴马表示，要确保网络安全，私人企业之间，以及私企同政府之间必须更快速地分享情报。“我们的许多电脑网络和关键基础设施都由私人企业界控制，这意味着政府不能孤军作战。事实是私人企业界本身也无法单独行事，因为最快截获威胁情报的向来是政府。”根据奥巴马的行政命令，国土安全部将拨款设立一个机构，制定有关自愿分享信息的标准。

（十三）《美国国防部网络战略》（the Department of Defense Cyber Strategy）

2015 年 4 月 23 日，美国国防部发布了《美国国防部网络战略》，这是 2011 年 12 月 12 日发布的《国土安全相关实体网络安全战略》的升级版。新战略明确了三大任务：一是保护国防部的网络、系统和信息；二是保卫美国国土及国家利益不受重大网络袭击活动的侵犯；三是集中网络军事力量支持军事行动和应急计划。战略提出了五大目标。

（1）建立和维持网络力量和能力以进行网络空间作战。

（2）保护国防部信息网络、确保国防部数据安全和减轻国防部任务风险。

（3）保护美国本土和美国切身利益免受具有严重后果的破坏性网络攻击。

（4）建立和维护可行的网络方案并在各阶段控制冲突升级以及塑造冲突环境。

（5）建立和维护强大的国际联盟以阻止威胁蔓延并增强国际安全与稳定。

奥巴马政府网络安全相关举措及行动路线图

美国历来十分重视网络安全，也是最早制定和实施网络安全战略的国家。从克林顿时代起，美国政府就将网络安全视为国家安全战略的重要组成部分。美国网络安全战略演变的实质，就是逐步确立美国的制网权战略。为保证网络安全战略的实施，美国形成了组织管理保障、技术保障、法律法规保障和执行保障等体系。经过克林顿和小布什两届政府，在国务院、国防部、情报部门、国土安全部等各部门的积极配合下，一个集战略思想、政策举措和行动策略三位一体的网络空间战略逐渐浮出水面。

奥巴马自 2009 年上任以来，比其前任更加强调网络空间安全的重要性，陆续发布了《网络空间政策评估》、《网络空间国际战略》、《网络空间行动战略》等一系列重要战略文件，为美国构建了一个立体的网络安全战略体系，也使网络安全成为美国国家安全战略的核心部分之一。在此框架下，美国政府相关部门采取了多项举措，重新安排网络空间的权力和规范，谋求更高程度的网络空间霸权，以确保美国政府所确定的繁荣、安全、价值观三大核心利益。

一、奥巴马政府对网络安全问题的整体判断和战略定位

（一）“最迫切的问题”、“最优先的事项”和“最严重的挑战”——进一步提升网络安全的国家战略地位

在竞选总统期间，奥巴马就表示要高度重视网络安全。2008 年 12 月，美国“第 44 届总统网络空间安全委员会”向当选总统奥巴马提交了《提交第 44 届总统的保护网络空间安全的报告》。报告指出，过去 20 年来，美国一直致力于设计一种战略，以应对网络安全挑战，保护美国利益，但始终都不算成功。网络安全以及信息基础设施在激烈竞争中受到攻击，削弱了美国的力量，使国家处于风险之中。报告明确表示：“美国不能保护网络空间，是新政府所面临的最迫切的国家安全问题之一”。奥巴马本人在竞选时，也曾批评小布什政府在解决网络威胁方面过于缓慢，并在 2008 年 7 月的一次讲话中称：“作为总统，我要让网络安全成为 2l 世纪的最优先事项。”就任总统后，奥巴马仍高度重视网络安全在国家安全战略中的作用，将其列为执政的首要任务之一。2009 年 5 月 29 日，奥巴马在公布网络安全审查和评估报告的演讲中称：“现在已经很清楚，网络威胁是我们国家所面临的最严重的经济和国家安全挑战之一。”并宣布“数字基础设施将被视为国家战略资产，保护这一基础设施将成为国家安全的优先事项”。

事实上，奥巴马上任以来推行的一系列网络安全举措，都可以从其上任之初的判断和表述中得到印证。结合其竞选期间的施政理念，奥巴马政府推行网络空间安全政策的动因可以概括为：适应国际环境变化，确保美国安全利益；维持信息技术优势，促进美国持续繁荣；运用新型网络力量，扩展美国价值观念。

（二）从网络防御、攻防结合到全球威慑——美国网络安全战略的“扩张性”演变

美国政府的网络安全战略，经历了从重视网络防御、网络攻防结合到全球网络威慑的演变。奥巴马执政以来，美国政府以《网络空间政策评估》和《网络空间可信身份国家战略》等文件为铺垫，以《网络空间国际战略》为典型代表，加上 2010 年 2 月的《四年防务评估报告》、同年 5 月的《美国国家安全战略》和 2011 年 2 月的《美国国家军事战略》等文件对网络安全及网络空间行动的指导与补充，奥巴马政府的网络安全政策体系日臻成熟。

奥巴马政府一系列网络安全举措的核心原则，体现在《网络空间国际战略》之中，即“基本自由、隐私和信息自由流动”。 具体而言，主要表现为经济、网络安全、司法、军事、网络管理、国际发展及网络自由七个领域的政策优先。纵观美国近三届政府的网络安全战略，先后经历了从保护美国关键基础设施到扩展先发制人的网络打击，再到谋取全球制网权的演变，明显体现出该战略的“扩张性”特征。

二、奥巴马政府推行的网络安全举措及行动路线图

鉴于美国垄断负责互联网运营的国际机构和企业这一现状，美国政府网络空间政策主要通过国际和国内两种行动策略来实施。

在国际层面，美国主要是推动一种“去政府化”的网络空间治理模式，一方面，从理论上把网络空间描述为“全球公域”，否认网络主权；另一方面，推动“多利益攸关方”治理模式，以企业、非政府组织、公民社会为网络空间治理的主体，限制国家及政府间组织在网络空间治理中发挥作用。此外，为进一步抢占网络空间治理领域的话语权，美国国务院牵头搭建“伦敦议程”（London Agenda）的网络空间治理平台，向其他国家兜售美国的思想和价值观。

在国内层面，奥巴马政府积极推动公私合作。美国的网络资源大多分布在政府之外的企业、非政府组织和社会当中，推动公私合作是为了整合这些资源，并将其转化为美国的网络权力。奥巴马政府还积极推动对于美国具有战略意义的网络技术发展，如大数据和云计算技术。对此，奥巴马政府特别责成白宫科技政策委员会成立大数据高层指导小组，要求联邦政府各部门积极支持“大数据研发计划”。美国政府不仅在每年庞大的 IT 采购预算中优先采购云计算服务，还建立联邦云计算示范工程，并通过一揽子计划鼓励亚马逊、谷歌、微软、IBM 等企业在全球获得领先地位，把美国打造成全球数据的存储、交换中心。这样一来，美国政府无须进入他国即可获得网络数据的“全球介入”能力。

具体到网络安全直接举措层面，奥巴马同样有着国内和国际的双重考量。对内，奥巴马确立了对网络安全问题的最高领导权，坚持推进美国数字化基础设施建设，呼吁政府和企业间的责任分享和有效响应，并加强了对网络行为的安全和隐私的保护。对外，奥巴马政府不断实行网络干涉，推行美国式的“互联网自由”，以互联网为工具直接干涉他国内政，并企图主导网络空间国际规则制定，从而确立其在网络空间的霸权地位。

（一）以国内为主线，巩固美国网络安全根基

为检验小布什政府的网络安全计划是否奏效，2009 年 2 月 9 日，奥巴马要求对美国网

络安全状况进行为期 60 天的全面审查和评估，并任命布什政府国家安全委员会主管网络安全的国家情报局局长顾问梅利莎·哈撒韦为牵头人，全面负责此项工作。同日，奥巴马政府公布将设立国家网络安全顾问一职，负责制定政策，协调联邦机构力量，并直接向总统报告工作。

2009 年 5 月 29 日，审查评估报告正式公布。报告主标题为“网络空间政策评估”，副标题为“确保可信任的适应性强的信息和通信基础设施”。报告内容包括：实施最高层领导，数字化国家能力建设，网络安全责任分享，建立有效信息分享和事件响应，鼓励改革创新，行动计划。并提出了近期行动计划 10 项和中期行动计划 14 项。

2009 年 3 月 10 日，美国国会研究服务局发布了《国家网络安全综合计划：法律授权和政策考虑》报告。报告指出，奥巴马政府的网络安全重点是继续加强行政和立法部门，国家和国土安全部门关注的首要威胁是对政府关键基础设施的网络攻击。同日，美国联邦审计署发布了《美国国家网络安全战略：需要进行的关键改进》报告，要求采取积极措施，进一步加强 5 个领域的网络安全，即支持网络分析和预警能力，完成网络安全实践提出的行动，增强基础设施控制系统的网络安全性，加强国土安全部对网络攻击的恢复能力，解决网络犯罪问题。2010 年 6 月 25 日，白宫宣布启动“网络空间可信身份标识国家战略”（NSTIC），建立综合身份标识生态系统框架。

2013 年 2 月，奥巴马发布了第 13636 号行政令《增强关键基础设施网络安全》，明确指出该政策旨在提升国家关键基础设施安全，并维护环境安全与恢复能力。2014 年 2 月，美国国家标准与技术研究所针对《增强关键基础设施网络安全》提出了《美国增强关键基础设施网络安全框架（V1.0）》，强调利用业务驱动指导网络安全行动，并按网络安全风险程度不同分为四个等级，组织风险管理进程。当日，美国国土安全部还推出了“C 立方”项目，即“关键基础设施网络领域志愿项目”进行配套建设，为所有自愿参考本框架的组织机构提供免费支持。

2015 年 1 月 22 日，奥巴马在其国情咨文中，将“隐私和网络安全”作为一项重要议题，提出了加大网络安全建设资金投入的提案，并在 2016 年财年预算报告中列出了该项目的改革目标，包括民营企业与政府的信息分享、反间谍功能的部署、网络教育的推广。2 月 12 日，奥巴马签署了一项旨在提高关键性基础设施网络安全的行政命令，要求美国政府与运营关键性基础设施的合作伙伴加强信息共享，共同建立和发展推动网络安全的实践框架。2 月 25 日，奥巴马下令成立“网络威胁情报整合中心”，旨在协调整合美国现有机构搜集的网络情报，进一步增强美国应对网络威胁的能力。

（二）以国外为力场，构建美国网络安全控制

尽管出于道德和国家形象的考虑，美国政府没有将对外网络干涉政策明确写入战略规划和政府报告，但从已有相关政府文件中依然可见端倪。事实上，网络干涉已成为美国网络安全政策一条隐藏的主线。

2011 年 5 月 16 日，美国白宫发布了《网络空间国际战略》，副标题为“互连世界的繁荣、安全与开放”。其战略意图明显，即确立霸主地位，制定规则，谋求优势，控制世界。同年 7 月，美国国防部发布了《网络空间行动战略》，提出五大战略措施，以捍卫美国在网络空间的利益，使得美国及其盟国和国际合作伙伴可以继续从信息时代的创新中获益。

2011 年 5 月 19 日，奥巴马发表了关于美国对中东和北非政策的讲话，提出美国致力于在中东和北非推动民主过渡和政治变革；政府的合法性取决于公民的知情权，美国政府必须支持互联网的自由开放，保护记者和博客作者的话语权。同年 7 月 14 日，美国国防部发布了《网络空间行动战略》，提出“国防部的国际行动将支持美国的《网络空间国际战略》以及美国总统在基本自由、隐私和信息自由流动方面的承诺”。

2013 年奥巴马进入第二任期以来，美国政府将网络力量再次整合改进，以服务于美国的外交目标。国务卿克里启用奥巴马上任之初的网络竞选精英以及白宫电子技术革新方面的人才，以让美国政府能够影响外国公众。2013 年 12 月 3 日，美国与爱沙尼亚签署关于网络伙伴关系的声明，提出两国在网络安全与网络自由方面开展合作，爱沙尼亚作为“自由在线联盟”的现任主席国，将与美国一起推进网络自由。

据美国《华尔街日报》2015 年 3 月 1 日报道，包括国务卿克里在内的美国内阁四名成员，联名致信中国官员，抗议中国银行业加强信息安全的新规，并且要求中国政府取消限制，以便外资科技公司进入中国敏感行业。4 月 1 日，美国总统奥巴马签署一项行政令，授权美国政府对参与“恶意网络空间活动”而危害到美国及公民利益的个人、组织和政府施加制裁。这项行政令给予政府新的权力，对于利用网络攻击威胁美国外交政策、国家安全和经济稳定的境外个人和组织，美国政府有权对他们采取制裁措施，包括冻结资产和限制入境等。

（三）奥巴马政府网络安全举措及行动路线图

美国《网络空间国际战略》报告最后提到，“此项战略是一个路线图，它使美国政府各部门和机构可以更好地界定和协调其在国际网络空间政策中的角色，按照特定的路线前进，并对未来如何贯彻该战略进行规划。”通过表 1.1 和图 1.1，可以更为清晰和直观地了解奥巴马执政至今，围绕网络安全推出的一系列文件、举措，以及其上任伊始提出的行动计划的推进情况。

表 1.1　奥巴马政府网络安全举措一览（2009 年至今）

时　　间	重要文件及举措	主要内容	相关措施跟进
2009 年 2 月 9 日	对美国网络安全状况进行为期 60 天的全面审查和评估	检查联邦政府各部门保护机密信息和数据的措施是否落实	
2009 年 2 月 26 日	奥巴马公布 2010 年财政预算，其中投资 3.55 亿美元用于加强美国公共部门与民营部门的网络安全	加强网络安全技术研发，支持“国家网络安全部”的日常运营及“国家网络安全综合计划”	
2009 年 3 月 10 日	美国国会研究服务局发布《国家网络安全综合计划：法律授权和政策考虑》报告	指出奥巴马政府的网络安全重点是继续加强行政和立法部门，国家和国土安全部门关注的首要威胁是对政府关键基础设施的网络攻击	
	美国联邦审计署发布《美国国家网络安全战略：需要进行的关键改进》报告	建议加强 5 个领域的网络安全，即支持网络分析和预警能力，完成网络安全实践提出的行动目标，增强基础设施控制系统的网络安全性，加强国土安全部对网络攻击的恢复能力，解决网络犯罪问题	

续表

时　间	重要文件及举措	主要内容	相关措施跟进
2009 年 3 月	美国国会提出专设“国家网络安全顾问”的议案	负责制定政策，协调联邦机构力量，并直接向总统报告工作	
	美国国土安全部通过一家网络技术服务公司招募网络安全人才	应征者应能“像恶意攻击者那样思考”，能够迅速判断政府网络系统的“薄弱之处”	在未来四年内，美国政府将提供 6000 万美元的资金支持
2009 年 5 月 29 日	奥巴马公布《网络空间政策评估：保障可信和强健的信息和通信基础设施》	实施最高层领导，数字化国家能力建设，共同承担网络安全责任，建立有效信息共享和事件响应机制，鼓励改革创新，提出近期行动计划 10 项和中期行动计划 14 项	
2009 年 10 月 30 日	美国国土安全部组建“国家网络安全和通信中心”	将网络安全的关注重点从军事应用领域全面推向国家层面	
2009 年 12 月 22 日	奥巴马正式任命网络安全专家霍华德 •施密特为美国网络安全协调官	统筹协调美国网络安全政策和行动	
2009 年年底	成立“全国通信与网络安全控制联合协调中心”	协调并整合六大网络安全专职机构的信息，提供跨领域的网络空间发展趋势判断能力，分析和报告全国网络空间的运行状况	
2010 年 3 月 2 日	对小布什政府制定的美国网络防御战略《国家网络安全综合计划》的部分内容进行了解密	通过建立和提高联邦政府内部对网络漏洞、威胁和安全事故风险的认识，最终通过各级政府和民营部门的合作，提高全社会果断行动、减少漏洞并预防入侵的能力	
2010 年 6 月 25 日	白宫宣布启动“网络空间可信身份标识国家战略”（NSTIC）	建立综合身份标识生态系统框架	（1）2011 年 1 月 7 日，美国商务部长骆家辉在斯坦福大学经济政策研究院透露，美国政府将寻求独立的网络技术供应商来设计、建造和提供网络身份识别技术，网络用户也可以自主选择是否拥有网络身份证 （2）联邦调查局在美国建立了 15 个“区域性电脑取证实验室” （3）2011 年 4 月，美国政府发布《网络空间可信身份标识国家战略》正式版
2010 年 9 月 28 日	美国国土安全部组织两年一次的“网络风暴-3”系列演习	首次通过真实的国际互联网实施演习，模拟推演美国联邦政府、地方政府、民营企业、关键基础设施网络等同时遭遇大面积“网络攻击”的场景	英国、法国、日本、澳大利亚等 12 个美国盟友共同参演

续表

时　　间	重要文件及举措	主要内容	相关措施跟进
2011 年 5 月 16 日	美国白宫发表报告《网络空间国际战略》	标志着美国互联网政策第一次有了顶层设计	
2011 年 5 月 19 日	奥巴马发表关于美国对中东和北非政策的讲话	提出美国致力于在中东和北非推动民主化过渡和政治变革，美国政府必须支持互联网的自由开放	
2011 年 7 月 14 日	美国国防部发布《网络空间行动战略》	支持美国的《网络空间国际战略》以及美国总统在基本自由、隐私和信息自由流动方面的承诺，制定五大战略措施	
2012 年 12 月	奥巴马签署第 20 号总统政策令《美国网络行动政策》	为“灵活”处理网络威胁，美军“可以动用独特的和非常规的能力”发动网络攻击和反击	
2013 年 2 月	奥巴马签署第 13636 号行政令《增强关键基础设施网络安全》	提升国家关键基础设施安全并维护环境安全与恢复能力	
2013 年 12 月 3 日	美国与爱沙尼亚签署关于网络伙伴关系的声明	提出两国在网络安全与网络自由方面开展合作	
2014 年 2 月 12 日	美国国家标准与技术研究所提出《美国增强关键基础设施网络安全框架（V1.0）》	利用业务驱动指导网络安全行动，并按网络安全风险程度组织风险管理进程	美国国土安全部推出“C 立方”项目，即“关键基础设施网络领域志愿项目”进行配套建设，为所有自愿参考本框架的组织机构提供免费支持
2015 年 1 月 22 日	奥巴马发表国情咨文	提出加大网络安全建设资金投入的提案，2016 年增投 140 亿美元	在 2016 年财年预算报告中列出改革目标，包括民营企业与政府的信息分享、反间谍功能的部署、网络教育的推广等
2015 年 2 月 13 日	美国政府在斯坦福大学举办网络安全与消费者保护峰会，奥巴马签署一项行政命令	鼓励民营企业与政府合作，共享威胁网络安全的信息	
2015 年 2 月 25 日	奥巴马下令成立“网络威胁情报整合中心”	协调整合美国现有机构搜集的网络情报，加强美国应对网络威胁的能力	
2015 年 4 月 1 日	奥巴马签署一项行政令，授权美国政府对参与“恶意网络空间活动”并危害到美国及公民利益的个人、组织和政府施加制裁	对于利用网络攻击威胁美国外交政策、国家安全和经济稳定的境外个人和组织，美国政府有权对他们采取制裁措施，包括冻结资产和限制入境等	

注：部分立法和网络战相关内容未涉及。

图 1.1　奥巴马政府网络安全行动计划路线图

三、奥巴马政府网络安全政策的特点

总而言之，奥巴马政府的网络安全政策具有如下特点：一是全局性和战略性。奥巴马政府将网络空间视为权力、财富、资源正在不断聚集，与“陆、海、空、天”同等重要的第五战略空间，并将网络空间“建章立制”视为与第二次世界大战后建立美国主导下的国际秩序同等重要。二是继承性和延续性。在小布什政府后期，美国已经开始探索建立在网络空间的

霸权，具有标志性意义的“奥林匹克计划”和“棱镜计划”正是在这一时期开始执行的。奥巴马上台后继承了上述项目并加大投入，其后来发布的多项网络空间战略，都未脱离前任政府的理念。三是控制性和进攻性。奥巴马时期的网络空间战略更强调控制性和进攻性，无论是积极发展网络军事力量，开展网络监控，还是推动网络空间的“建章立制”，都是在采取进攻性的手段，实行对网络空间中权力、资源、财富的控制。

（一）以完善领导指挥体系为着力点，全力加强美国政府在网络空间的统筹协调能力

奥巴马政府认为，美国政府网络空间安全机构存在着战略重心不明、职能重叠、缺乏协调配合等问题，因此必须从最高层实施领导，全面协调网络安全机制。2009 年 5 月，白宫宣布组建网络空间安全办公室，负责为总统提供网络空间安全方面的决策方针，协调政府相关政策与活动。并由此打造了一体化的综合性国家网络安全领导体制：在网络空间安全办公室统一协调下，国土安全部主管政府机构、社会团体、大型企业等的网络安全政策及其实施与保障；网络空间司令部负责军方网络安全政策和网络战指挥。通过建立新机构和划分职能，美国政府在网络空间的全盘统筹和协调水平得到了提升。

（二）以网络空间安全威胁为借口，始终高度重视对关键基础设施的防护

“威胁”可谓是美国网络安全政策中出现频率最高的词汇。美国认为，自己在网络空间中正面临着一场新的看不见硝烟的战争，且已处于劣势，其原因有三：一是美国的社会运转对计算机网络的依存程度远超过全球平均水平；二是美国认为自己的网络空间安全战略、安全观念和机制已不适应形势的发展变化；三是网络本身的松散结构决定了其薄弱环节众多，且网络空间进入门槛低，攻击技术和工具易于获取，而防范技术发展则相对滞后。基于上述原因，奥巴马上台后不断强调把网络安全作为国家安全战略的一部分，把网络从基础设施上升为战略资产加以保护。可以说，美国所有网络空间安全政策都是以此为出发点出台和实施的。

（三）以强调国际网络空间合作为手段，力求掌控全球网络发展主导权，维护美国霸权地位

奥巴马政府之所以一改美国多年来的抵制态度，高调宣传网络空间国际合作，一方面在于其认识到，即使美国这样的超级大国，也不可能凭一己之力解决网络空间存在的诸多问题，更重要的是美国希望利用自己雄厚的互联网资源，通过在网络空间的国际行动掌控全球网络发展主导权，改变和影响其他国家的政治体系和价值观念，巩固自身的霸权地位。奥巴马政府通过开展全民网络外交，使大批美国官员、学者和公民社会组织参与到美国政府领导下的价值观网络推广和意识形态渗透行动之中，外交、军事、传媒和法律等手段都被充分整合利用，形成了从宏观到微观的多层次、多渠道网络干涉手段。

四、对奥巴马政府近期网络安全政策走向的分析和预期

奥巴马政府在第一任期内完善了网络安全的制度建设和机构建设。美国政府通过重视关键网络基础设施的保护，不仅提升了民众的网络安全意识，而且有利于政府与民营机构间的

合作。在奥巴马第二任期内，美国政府努力促进与民营企业的合作，希望增强企业遵守政府法令的积极性。为了巩固在网络空间的领导地位，美国不仅加强自身的网络部队建设，而且与盟国及伙伴国的合作进一步深化。然而，美国的网络安全政策面临一系列挑战。“斯诺登事件”对美国的网络政策产生了负面影响，美国提倡的网络空间国际规范也遭到与美国价值观不同的国家的质疑。鉴于国际形势和美国实力的变化，奥巴马在其第二任期内的网络安全目标推进缓慢。

随着互联网的进一步发展，网络安全在美国国家安全战略和全球战略中的地位变得更为重要。相比第一任期，奥巴马第二任期的网络安全政策力图推进完成现有的政策目标，表现出施政理念的完整性；同时将在国际网络安全问题上更具进攻性，以确立美国网络空间霸权地位。

（一）新瓶装旧酒——关键性基础设施防护的重点政策仍将延续

2015 年以来，奥巴马在网络安全方面动作频频，不仅就网络安全问题提出了立法建议，还签署了行政命令呼吁企业与政府分享网络安全信息。然而与此同时，不时有美国机构和企业声称用户数据等遭黑客窃取。据统计，网络威胁每年给美国经济造成的损失达到经济总量的 0.1%～0.5%。仅在 2012 年，美国经济因商业机密遭窃取就损失了 3000 多亿美元。美国社会加强网络安全的呼声高涨，奥巴马因此计划持续推出新政以应对网络威胁。虽然在美国关键性基础设施面临的严峻网络威胁面前，奥巴马网络安全新政的效果仍未得到充分体现，并被视为往届政府政策的“翻版”，但评估奥巴马以往推出的举措，加上 2015 年以来提出的网络安全新政，都可以预期其将不遗余力加强网络安全建设，以完成历届美国政府设定的目标。

（二）后“棱镜门”时代——美国网络空间政策走向政治化、意识形态化和军事化

奥巴马政府的网络空间战略是一个复杂而矛盾的体系，其既要维护网络空间开放、透明、可操作性，又要建立美国的网络霸权；协调机制不畅，导致国务院、国防部、国土安全部及情报部门的政策之间相互抵触甚至抵消；国际和国内层面的行动策略彼此冲突。“棱镜门”事件更加速了矛盾的爆发，暴露出奥巴马政府过度推进进攻性网络政策、开展网络监控、干涉他国主权和垄断互联网管理权，把网络空间推向了政治化、意识形态化和军事化的困境。未来，美国的网络空间战略面临国际和国内的多重挑战。首先，在国际上陷入信任危机。美国一直把建立网络空间的“行为规范”标榜为其网络空间国际战略的主要目标之一，但在斯诺登披露“棱镜计划”之后，各国均将美国这一“规范”视为加强控制的举动，而这一质疑极有可能难以消解，最终形成对立。此外，美国的网络监控行为侵犯了美国民众的隐私权，与公民言论自由相悖，也对美国现有的司法制度形成了挑战。

（三）网络空间霸权的导向作用——最终真正占据网络安全的制高点

奥巴马政府分别于 2009 年和 2011 年发布了《网络空间政策评估》和《网络空间国际战略》，对外公布了美国在网络空间的战略思想和战略目标。奥巴马政府认为，发展中国家在互联网治理论坛和国际电信联盟这两个平台中数量占优，而且更支持“网络主权”，于是采

取各种措施抵制其发挥作用，并于 2011 年创立“伦敦议程”，试图以此主导网络空间治理进程。美国控制着全球互联网的主根服务器和信息流节点，掌握着全球互联网管理规则的主导权，但是奥巴马政府并未满足于这些优势，而是通过网络干涉在网络的外交运用方面赢得先机和垄断权，将网络干涉从点到面逐渐铺开，形成宏大的全球网络控制体系，巩固美国的网络霸权地位。

当今世界，美国的对外网络干涉政策引发了一系列后果，影响着网络空间的未来发展和各国网络政策。首先，一些国家和非政府组织可能模仿美国，从而使网络空间可能面临更严重的失序。其次，网络干涉政策更加暴露了美国在网络问题上的“双重标准”，加剧网络空间的不公平现象。最后，网络干涉政策严重侵犯他国主权和公民隐私，容易引发国际争端。总体而言，美国网络干涉激化了国际信息领域的矛盾，导致“网权”争夺更加白热化，全球网络治理将面临更大挑战。

美国关键基础设施网络安全保护的经验分析

一、背景：日益严峻的关键基础设施威胁

随着物联网、大数据的发展，越来越多的关键基础设施之间实现互联互通，并接入了广袤的互联网。这一方面释放了经济发展的潜在活力，另一方面让市场运行越来越依赖于基础设施的智能化。随之而来的是“新的脆弱性”，例如，“设备故障、人为错误、天气及其他自然灾难以及物理和信息攻击”，尤其是关键基础设施联网后所面对的无处不在的潜在网络攻击威胁。

2010 年的“震网”事件表明，美国已经掌握了可以快速致瘫他国关键基础设施的网络攻击能力。但是，由于美国对于信息系统的高度依赖，其本国的关键基础设施面临的网络安全风险也远高于大多数国家，只要有一点点安全漏洞，就足以造成巨大的经济损失。“9 •11”事件爆发后，美国对本土安全和关键基础设施的重视程度大幅提升，历任美国政府都在保护关键基础设施、提升网络安全方面推出了相关政策。2015 年 2 月，美国颁布新的《国家安全战略》，明确将针对美国本土或者关键基础设施的毁灭性攻击列为影响本国利益的最高战略性风险，对于网络空间也明确了美国必须发挥“领导地位”。经过多年的谋划和经营，美国关键基础设施保护已经形成了一系列比较成熟的做法，分析和研究其相关政策沿革，有利于为我国关键基础设施保护提供相关政策经验作为借鉴与参考。

二、美国关键基础设施保护的相关情况

（一）美国关键基础设施保护的政策沿革

1. 克林顿执政期：保护机制雏形初成，首提公私合作

1995 年 1 月，克林顿总统发布了关于反恐怖主义政策的总统令。根据这一命令，司法部成立了关键基础设施工作组，研究美国关键基础设施所面临的风险和威胁。

1996 年 7 月，克林顿政府颁布了第 13010 号行政令《关键基础设施保护》，初步划定了关键基础设施的范围，宣布成立关键基础设施保护机构——“总统关键基础设施保护委员会”（PCCIP），负责开展关键基础设施薄弱环节及其面临的威胁研究，就制定相关政策规划提出建议。同年，克林顿接连签署了两份对第 13010 号行政令进行增补的文件，分别为第 13025 号行政令和第 13064 号行政令。

1998 年 5 月，美国政府颁布了第 63 号总统令《克林顿政府对关键基础设施保护的政策》，分析了关键基础设施的脆弱性，指出对关键基础设施和信息系统的非传统攻击会严重危害美国的经济和军事，强调政府和私人部门合作保护基础设施的重要性，并确定了保护关键基础设施的部门分工，同时计划成立国家基础设施保障委员会（NIAC）和关键基础设施协调组（CICG），以加强关键基础设施保护中公共和民营部门间的合作关系，并在必要的时候向总

统提交报告。该总统令还要求在联邦调查局设立国家基础设施保护中心（NIPC），用于评估潜在的威胁并发布预警信息。

在克林顿执政期间，关键基础设施涉及的领域和范畴得到明确。1996 年克林顿总统第 13010 号行政令将关键基础设施分为电信、电力、天然气及石油的存储和运输、银行和金融、交通运输、供水系统、紧急服务（包括医疗、警察、消防、救援）、政府延续性八类。在第 63 号总统令中，其定义得到进一步厘清，“关键基础设施是指那些物理系统和以计算机、网络为基础的系统，它们对于最基本的经济运行和政府运转非常关键。”

围绕关键基础设施保护的目标、行动策略以及行动计划的时间表也制定完成。就目标而言，第 63 号总统令指出，“最迟不晚于 2000 年，美国应当实现初步的信息保障能力；从这份总统令发布之日起，五年后（2003 年）美国将具备并保持对我们国家的关键基础设施进行保护的能力。”就行动策略而言，要密切协调公共和民营部门的工作，其中政府部门应设立“部门联络官”，民营部门应指派“部门协调员”，最大限度地降低合作的行政和资金壁垒。就制定行动计划及其时间表而言，第 63 号总统令明确指出要制定政府和民营部门的“国家基础设施保障计划”；同时，计划总统令发布后 180 天内，由 CICG 首脑委员会（Principals Committee）制定并完成国家基础设施保障计划的日程表，具体包括脆弱性分析、矫正计划、预警、响应、重建、教育和意识培养、研究和开发、情报、国际合作、立法以及预算要求。

按照第 63 号总统令的要求，2000 年 1 月，美国政府出台了《保护美国网络空间：保护信息系统的国家计划》。这一计划是全球首次由国家政府实施、用来设计其国家网络空间保护方案的尝试性活动。计划进一步重申了公私合作的必要性，“民营企业的基础设施至少也是网络攻击的目标。在现代社会，关键的工业和公用事业已经成为各种冲突的破坏目标。美国的国力就在于私人所拥有和运作的诸多关键基础设施和工业。”为了支持政府部门与民营部门的计划的制定，政府还将成立关键基础设施保障办公室（CIAO）。这一合作机制也将延伸至关键基础设施保护的研发环节，通过政府、民营部门、学术界共同合作，更新每年政府关键基础设施保护研发项目的优先级。另外，还将在个体和民营企业、州政府和地方政府、联邦政府之间建立对威胁的共识和应急响应机制。

2. 小布什执政期：保护文件密集出台，清晰界定保护范畴

2001 年的“9 • 11”恐怖袭击事件让刚刚上台的小布什总统深刻意识到保护关键基础设施的重要性和紧迫性。当年 10 月，小布什正式签署了《爱国者法案》，重新界定了关键基础设施，并提出了建设关键基础设施建模、方针和分析系统的保护措施。接着，他发布了第 13231 号行政令《信息时代的关键基础设施保护》，宣布成立“总统关键基础设施保护委员会”（PCIPB），取代 PCCIP 代表政府全面负责国家的网络空间安全工作。

2002 年，小布什政府公布了《网络空间国家安全战略》（草案版），这成为全面加强美国的国家信息安全战略规划的纲领性文件。2003 年，该战略的正式版本对外发布。依据同年生效的《国土安全法》的规定，小布什总统组建国土安全部，统筹关键基础设施的保护措施。

2003 年，小布什政府出台了关于关键基础设施保护的两份重要文件：《关键基础设施和重要资产物理保护国家战略》和第 7 号国家安全总统令《关键基础设施标识、优先级和保护》。前者提出了“重要资产”这一概念，明确了政府和民营部门的职责；后者为政府各部门和相关机构确定了保护关键基础设施免受恐怖主义攻击的工作目标。

2006 年 6 月，国土安全部发布《国家基础设施保护计划》，概述了国家基础设施保护工作的任务职责、风险评估策略、教育培训等。

2007 年 5 月，小布什政府发布《关键基础设施和重要资产部门分计划》，确定了分领域的安全目标，明确了财产、系统、网络数据和功能鉴定等事项。

这一阶段是关于关键基础设施保护的政策文件密集出台的阶段。关键基础设施的分类体系愈加完善，相关的组织结构也更加集中。到 2008 年，小布什政府共明确了 18 类需要保护的关键基础设施和重要资产，分别为农业和食品、能源、公众健康和保健、电信、邮政和运输业、交通系统、化学、商业设施、政府设施、紧急事务处理部门、水坝、核反应堆、原料和垃圾、国防工业基地、国家纪念性和标志性建筑，以及关键制造业等。2002 年成立的国土安全部将分散在联邦调查局、国防部、商务部等各机构的基础设施保护机构吸纳至其下属的信息分析与基础设施保护局，以期降低协调成本，实现统筹计划、应急响应和技术援助全方位保护工作。

这一时期，关键基础设施保护的公私合作也上升到新的台阶。2002 年《网络空间安全战略》重申了民营部门和社会团体是实现国家安全保护的重要力量。2003 年的《关键基础设施和重要资产物理保护国家战略》概述了美国关键基础设施具有高度的复杂性和异质性，因此，联邦政府、州及地方政府、民营部门之间应建立前所未有的合作，在风险评估、保护预案、具体举措方面建立信息共享及协作机制。

3. 奥巴马执政期：保护体系日渐完善，重申私企合作重要性

奥巴马政府不仅把网络列为关键基础设施，而且把它升级为国家战略资产，是国家安全与经济的命脉。2009 年 2 月，奥巴马政府公布“国家基础设施保护计划”，要求美国联邦政府、州政府、地方政府与民营企业合作，全力保护网络安全。奥巴马在 2009 年 5 月公布《网络空间政策评估报告》时谈到，美国 21 世纪的经济繁荣将依赖于网络空间安全。他将网络空间安全威胁定位为“美国面临的最严重的安全挑战之一”，并宣布“从现在起，我们的数字基础设施将被视为国家战略资产。保护这一基础设施将成为国家安全的优先事项”。2009 年美国《国家情报战略》把反情报工作和维护网络安全确定为情报部门未来 4 年的两大重点，而且反情报工作要在“整个互联网范围内”开展，以“保护关键性基础设施”。

2013 年 2 月，奥巴马签署了第 13636 号行政令《增强关键基础设施网络安全》和第 21 号总统令《提高关键基础设施的安全性和恢复力》。行政令提出要建立政府与民营机构的信息共享机制，授权由美国商务部牵头、国土安全部配合，指导美国国家标准与技术研究所（NIST）制定降低关键基础设施信息与网络安全风险的框架。总统令进一步明确了政府相关部门的职责，梳理了关键基础设施名单，厘清了关键基础设施保护中政府和企业的关系，力争形成合力，优化信息共享和责任共担机制。

2014 年 2 月，白宫宣布发布由 NIST 经过多次修订形成的《提高关键基础设施网络安全框架》第一版。该文件从识别、保护、侦测、响应和恢复五个层面制定了美国关键基础设施信息安全防护体系框架，贯穿了机构组织网络安全管理的全周期。文件从初始级、风险预警级、可重复级和自适应级四个层级描述了企业进行网络安全风险管理的推进过程。其中，自适应级是组织网安管理的最高级别，可积极适应变化的网络安全形势，及时应对日益复杂的安全威胁。

2015 年 2 月，白宫成立网络威胁与情报整合中心（CTIIC），该机构将协调整合国土安全部、联邦调查局等多部门的情报力量，提高美国防范和应对网络攻击的能力。为保护美国公民网络信息，该机构还将与美国企业保持紧密合作，推动政府与企业信息共享。同月，白宫还发布了《促进民营部门网络安全信息共享》行政令，宣布在民营部门自愿的基础上，鼓励民营部门和公共部门一道建立网络威胁信息共享和分析组织，从而更好地处理威胁到公共卫生和安全、国家安全及经济安全的网络威胁。

2015 年 4 月，美国国防部发布《网络战略》，从更加广义的网络与美国国防部职能之间的互动关系出发，提供网络安全问题的战略性指导。该战略突破了“军民两分”原则，相比以往，更强调用美国网军司令部的力量保障美国民间的网络关键基础设施，并且明确介入关系美国国家利益的“民用”网络空间。

（二）美国关键基础设施网络安全保护的三大基石

1. 信息共享

保护关键基础设施的网络安全，关键在于明确关键基础设施的脆弱性，对可能遭到网络攻击和出现的网络漏洞提前预警。预警的有效手段之一就是所有关键基础设施行业的信息共享机制。美国历届政府发布的政策指南中，都会开辟专门的章节强调信息共享的重要性和具体策略。例如，奥巴马第 13636 号行政令中称，“通过保证大容量、及时和高质量的网络威胁信息共享来保护美国政府与民营部门免受网络威胁。”

2. 公私合作

这主要是基于以下几方面原因的考虑：第一，民营部门是国家关键基础设施和服务的重要提供者。一旦发生网络安全事件，与民营部门的合作，有助于迅速找到网络威胁的源头，并恢复正常的秩序，降低网络安全事件造成的损失。第二，民营部门是国家关键基础设施的所有者或运营者。美国 85%的重要基础设施归民营部门所有或运营，这些基础设施如电信、能源、交通等往往容易成为外国恐怖分子或敌对势力的网络攻击目标。因此，民营部门对保护公众安全和维护国家利益具有不可推卸的责任和义务。此外，网络安全造成的损失也会危及民营部门所有者或运营者自身的利益，与政府部门的合作也与保障其自身利益密切相关。第三，部分运营关键基础设施的民营企业对网络安全保护的意识或能力有所欠缺。据卡巴斯基实验室负责人介绍，电力网络、供水系统、化工厂等关键基础设施企业搜集网络安全威胁的设备陈旧，改进措施不及时，甚至与一般企业相比，它们在基础设施升级方面更加缓慢。

3. 隐私保护

美国从克林顿时期的关键基础设施保护的文件起，都会专门强调基础设施网络安全的保护要以与公民的自由权利益保持一致为前提，力求每一份政策文件和相关举措都包含了对美国公民的自由权和隐私权保护的内容。同时，对与美国政府合作的民营企业，美国政府也一贯遵循自愿的方针，让企业自愿加入网络安全保护的计划中，并对民营企业自愿提供的资源和信息，予以法律许可范围内的最大限度保护。

（三）美国政府促进关键基础设施保护公私合作的障碍

美国政府在统筹关键基础设施保护方面遇到的最大难点就在于如何让更多民营部门自

愿地采纳国家制定的关键基础设施保护计划和网络安全框架。由于民营部门不是国有资产，因此，美国政府将其纳入网络安全战略，成为一个完全全力合作力量并不现实。

首先，民营部门与政府部门之间存在博弈。美国政府部门期望拥有更多的权力处理民营部门的网络安全问题，甚至连奥巴马总统也在敦促国会就这一方面以立法的形式确立下来，但是，这一举措一直遭到民营部门的反对，与此相关的网安立法工作则处于停滞状态。

其次，民营部门对隐私保护的诉求更强烈。美国政府希望能够更多地掌握民营部门手中海量的数据资源，然而，考虑“斯诺登事件”曝光后的负面影响，民营部门对是否为美国政府提供数据以及提供哪些数据方面的决策更加谨慎，以期在公众中和国际上保护公开透明的企业形象。

最后，民营部门非常担忧与政府合作的法律责任。美国网络司令部司令迈克尔·罗杰斯认为，这一担忧是可以理解的，为了解决这一问题，双方需要明确界定事先共享哪些信息。在他看来，“隐私信息”不是网络安全的重点，因而不应成为任何信息共享协议的一部分。他认为，关键环节在于对话沟通。

三、对我国关键基础设施保护的启示

首先，加快构建关键基础设施网络安全保护的法律体系。美国围绕着网络安全保护已通过多部法律，明确了联邦政府及各机构在网络安全保护方面的责任。一份有关确定信息提供规则的法律《美国自由法案》即将生效。同时，美国历届政府都会制定多个行政令和总统令，进一步明确关键基础设施保护的责任、流程和机制。因此，随着我国工业 4.0 的开展和“互联网+”的升级，关键基础设施保护迫在眉睫，亟须建立关键基础设施网络安全保护的法律体系，从法律层面明确关键基础设施的定义和范围、界定政府部门的职责、规范运营者和所有者的运营资质要求。

其次，明确对关键基础设施进行分类分级。关键基础设施数量众多，其重要性和潜在的破坏力也不尽相同，有必要划分关键基础设施信息安全风险等级，并对其进行分级管理。因此，应尽快制定关键基础设施网络安全风险分级规范，根据关键基础设施的重要性、影响范围、网络攻击的可能性等因素，提出界定关键基础设施信息安全风险等级的量化标准，分级制定管理要求。

最后，建立政府和企业间紧密的合作关系。与美国不同，我国的关键基础设施和重要资产绝大多数都掌握在国家手中。因此，我国在保护这些基础设施中，中央政府可协调的资源更多，政策的执行力度将更大。不过，由于我国的关键基础设施都是垄断性行业，因此，基础设施的投资渠道单一，容易造成基础设施建设落后，企业在关键基础设施网络安全保护的意识和举措方面不到位。因此，一方面，政府应当加强对关键基础设施企业的网络安全指导，明确各自的职责；另一方面，政府应当鼓励企业建立更多的激励机制，让企业根据自身情况构建适合自身发展的网络安全保护框架。

美国强化网络空间霸权以加强对全球的控制

互联网时代，传统国际政治领域的主导权争夺已延伸至网络空间。美国政府近年来大力谋求网络空间的主导地位。这既是美国全球霸权战略的重要组成部分，也对其全球霸权的实现起到了重要支撑作用。

一、美国多管齐下加强网络空间战略基础建设

（一）加强网络空间战略体系及顶层规划以抢夺网络空间战略制高点

美国的网络空间战略经历了一个由“被动保护”到“主动出击”的渐进发展完善的过程。自克林顿政府伊始，美国网络空间战略从“保护”敏感信息与数据、关键系统及基础设施安全，逐渐过渡到侧重“监控”信息内容，最终发展至奥巴马政府推崇的“积极防御”潜在威胁、“塑造”有利于美国的世界网络环境，将目标直指全球网络空间。

奥巴马政府以多项政令推进其侧重“对外控制”的网络战略。2009 年 5 月，奥巴马政府发布了《网络空间政策评估》，强调美国 21 世纪的经济繁荣将依赖于网络空间安全。2011 年 5 月，奥巴马政府发布了第一份明确表达主权国家在国际网络空间中的行动准则的战略文件《网络空间国际战略》，成为美国国家网络安全战略的集大成者，其出台标志着美国国家网络安全战略的整体定型。该战略集中体现了美国主导网络空间的意图：经济方面，推动国际标准和创新、开放市场的建立；网络安全方面，加强网络的安全性、可靠性和灵活性；司法方面，拓展合作与执法力度；军事方面，加强应对网络威胁的能力和国际合作；网络管理方面，建设有效和包容的管理结构；网络自由方面，支持基本自由和隐私。此后，国防部依据该战略发布了《网络空间行动战略》，创造性地提出了“积极防御”概念，显露出其“以战止战”、“先发制人”的思想，集中体现了美国网络战略的对外控制性。2012 年 12 月，奥巴马签署了第 20 号总统政策指令《美国网络行动政策》，详细规定了美国在网络空间采取进攻性和防御性网络政策的原则、目标和方案，显露了美国在网络空间建立霸权的本质，对其整个网络政策体系导向产生了重要影响。

可以看出，美国的一系列网络战略文件旨在整合网络的经济、政治、外交、社会功能，竭力宣传“网络自由”主张；同时全力维护和巩固其网络优势，阻碍建立国际网络治理新秩序；其确立的主动出击的战略思想，更是直接暴露了强烈的网络霸权意图。

（二）强化网络空间战略机制建设以强化网络空间霸权基础

为保障网络战略的顺利执行，美国多个政府部门参与了网络战略推进。同时，通过不断完善部门沟通机制，美国建立了较为先进的网络战略推进体系。

美国网络国际战略的主要执行部门是国务院，其职责在于利用外交手段积极推销在网络空间的价值观，强化盟友之间的价值观同盟，并通过网络空间“建章立制”，试图建立起一套符合美国利益的网络空间规则。同时，美国多个职能部门也建立了相应的网络战略

保障机构，如隶属国土安全部的“美国计算机应急响应小组”，隶属国防部的“联合作战部队全球网络行动中心”和“国防网络犯罪中心”，隶属联邦调查局的“国家网络调查联合任务小组”，隶属国家情报总监办公室的“情报系统网络事件响应中心”，隶属国家安全局的“网络空间安全威胁行动中心”。而最能代表美国网络战略对外扩张性的，则是 2010 年 5 月组建的网络战司令部，该机构整合了分散于多个部门的网络力量，下设多达 541 个下级司令部，64 个网络战空军中队、预备役和国民警卫队，4 个空军网络战联队和陆海军网络战部队，将情报、进攻和防御融为一体，集组织、培训和装备网战部队，实施网络攻防战等职能于一身。

同时，美国建立了较为顺畅的联系机制，保障网络战略部门的纵向和横向沟通。为了加强各职能部门与白宫的联系，美国设立了与总统保持密切联系的“白宫网络安全协调员”，并成立了“白宫网络安全办公室”，协调美国联邦政府所有军事和民事部门网络安全政策和行动。2009 年年底成立的“全国通信与网络安全控制联合协调中心”，意在协调和整合各大网络安全专职机构，形成一体化的综合性国家网络安全领导和协调体制。此外，各部门之间也开展了一系列横向协作，如国防部与国土安全部签订了“2010 协作备忘录”，增加在政策法规、任务成效和预算三方面的合作；国土安全部、司法部、国家安全局等通过加强协作，制定网络安全框架、行动指南和工作程序，维护美国关键基础设施的网络安全。

（三）推出“网络自由”战略理念以为网络空间“建章立制”

“网络自由”思想是美国全球战略的信息化辅助手段和信息心理战措施，发挥着日益重要的作用。从 2010 年起，由国务卿希拉里主导的美国国务院逐渐形成和完善了“网络自由”的概念。通过对全球网络空间环境的塑造，将全球网络空间和最新的互联网应用作为实践美国外交政策的新工具。同时，希拉里通过两次“网络自由”演讲在全球范围内大肆鼓吹该思想，宣扬所谓虚拟世界的“公开、透明和人权”，称美国将把“不受限制的互联网访问作为外交政策的首要任务”，“要使互联网能够经受跨越网络、边界和区域的各种形式的干扰而始终保持通畅”。

“网络自由”概念统领了美国互联网国际战略的整体性框架，即《网络空间国际战略》。同时，作为该战略的七个“政策重点”之一，“网络自由”被反复强调：“美国鼓励全世界人民通过数字媒体表达观点、分享信息、监督选举、揭露腐败、组织政治和社会运动”，“美国将继续确保网络全球化带来的好处，反对任何国家将网络分裂为本国内网，剥夺个体接触外部世界的企图”。

“网络自由”的概念是由美国为整个国际社会定义的。经由对美式“网络自由”主张的推行，并使其成为“国际标准”和“世界共识”，美国可以进一步掌控网络空间的国际话语权。首先，美国通过提出“网络自由”占得先机，巩固和强化其在国际网络空间规则制定上的主导地位。其次，要求国际社会遵守“网络自由”规则，利用网络的虚拟性打破传统意义上的国界线和主权边界，为更大程度上实现美国国家利益做铺垫。最后，通过“网络自由”思想，美国可以将自身标准强加于国际互联网空间，为干涉其他国家内政提供依据和口实。“网络自由”看似简单的互联网概念界定和运行规则主张，实则透露出美国的整体战略考量。

二、美国利用网络空间霸权强化全球控制的具体表现

（一）在政治意识形态方面，利用互联网对外进行政治引导及价值观输出

利用信息霸权进行意识形态扩张，已经成为当今美国意识形态外交的重要手段。互联网上信息相对自由的流通与传播，也是美国进行意识形态扩张的有效途径。以对我国意识形态输出为例，网络就被美国赋予了“扳倒中国”的重要功能。美国前国务卿奥尔布赖特曾说：“我们要利用互联网把美国的价值观送到中国去。”

综合美国近几年的动作来看，其主要通过以下几种手段进行网络意识形态输出。

一是利用网络平台诋毁其他国家，同时传播美式价值观，改善美国国家形象。全球网络空间处于极度不平衡的状态，美国拥有绝对的网络传播优势，其利用信息不对称，强制性地对外输出其美式价值观。如美国近年来大肆炒作“中国威胁论”，通过互联网载体对我国政府工作中的不足夸大其词、横加指责，坚持从西方价值观角度来解读我国政策等，从而达到弱化我国网民的国家认同和政治认同的目的。

二是强调“网上民主和人权”，意图为其意识形态输出打开缺口。美国近年来大力兜售“网络自由”思想，强迫其他国家屈服，迫使其他国家开放互联网管制禁区。同时，为了争取国外民间支持，大力向民众尤其是青年提供廉价甚至免费的网络工具和上网便利，鼓动他们“网络问政”，积极宣扬“网络民主”，逐渐培养其对美式“网络自由”理念的认同。这一形式最具有代表性的就是美国通过网络服务解禁等方式，源源不断地对中东进行网络意识形态渗透，最终触发和催化了 2011 年中东地区的政局动荡。

三是多方出击，形成网络政治输出合力。美国政府策划和主导，学术界、商界和非政府组织多方协同参与、共同组织实施网络外交，按照自身的标准筛选和推出符合其价值标准的互联网信息内容及传播方式进行传播活动。同时处心积虑地为目标国家的反对派提供信息技术支持，为他们普及现代网络通信工具的使用，强化组织联系沟通和信息交换，提高政治组织的运行效率和政治影响。

（二）牢牢掌控网络空间“制网权”，利用互联网技术资源优势对外发起技术攻击与破坏活动

作为互联网的发源地，美国在网络技术和网络资源分配方面都占据着绝对优势。目前，全球有 13 台域名根服务器、1 台主根服务器和 9 台副根服务器设在美国，其余 3 台分别在英国、瑞典和日本。美国控制着被称为“全球互联网中枢”的 ICANN，也就控制了别国互联网的命门。同时，网络通信协议、核心技术、计算机芯片、基础软硬件等也多由美国主导提出或研发。网络空间在一定程度上可称为美国的“后花园”。

美国凭借其技术优势牢牢掌控“制网权”。一是不断加大投入，技术输出规模不断扩大。自 2013 年投入 103 亿美元以来，美国用于网络安全的资金投入近年来呈稳步增长趋势，预计 2016 年将达 140 亿美元。在源源不断的资金支持下，美国的网络技术输出已进入从小项目小投入到大项目大投入、从个别政府部门项目到国家战略项目、从在重点国家和地区推广到全球普遍部署推广的新阶段。如近年来美国推行“无线未来计划”、“开放技术计划”等技术项目，为其未来技术控制做好铺垫。二是凭借技术优势对别国进行“镇压”。美国近年来

重金研发“破网”技术，为的就是压制别国的网络技术对抗，侵蚀他国网络和通信空间。如美国启动的“影子互联网计划”、“弹弓计划”等项目，可绕过主权国家官方网络监管系统，向目标受众传播被屏蔽内容。同时，美国政府资助互联网公司、非营利组织等的“翻墙”项目，加强与他国网络管制的技术对抗。如西亚和北非发生政局动荡后，美国国务院向互联网和软件公司注资逾 2000 万美元，帮助网民突破政府网络过滤。三是直接进行网络监听。从理论上说，美国凭借对根服务器的掌控和其无可比拟的技术优势，能够轻易地进行全球性的情报窃取、网络监控和攻击。事实亦是如此。斯诺登爆料显示，美国对多个国家实施了监听，谷歌、雅虎、微软和 Facebook 等网站的服务器成为美国政府获取信息的重要途径；仅“X key score”计划就通过在全球的 150 个站点和 700 台服务器展开了全球性网络监控；监听终端包括计算机、手机 SIM 卡、邮箱系统等；监听内容包括文字、语音、视频。更为重要的是，美国利用发达的技术进行精确定位，多国领导人、别国重要部门都成为其为监听对象。

美国的网络霸权，主要表现为技术上的霸权。利用在计算机和网络信息领域的绝对技术优势，美国在国际行动中掌握更大的主动权，将技术优势转为战略优势，谋求实际利益。

（三）强化互联网经济霸权地位，利用硅谷在互联网技术应用方面的优势，主导和控制全球互联网市场

随着互联网与经济的密切结合，美国也开始在互联网经济领域建立霸权地位，妄图通过控制互联网市场来影响甚至控制其他国家的经济，进而达到其不可告人的目的。

美国通过互联网对他国的经济干预，主要从两个方面进行。一是凭借其强大的互联网经济体系，占领他国市场。在社交网络、搜索引擎、邮箱等互联网产业领域，美国都占有主导地位。以谷歌搜索引擎为例，其在美国境内的市场占有率约为 67%，而其在欧洲、亚洲部分国家的市场份额则高达 90%，甚至 95%（如德国）。即便在互联网管制较为严格的国家，其市场份额也不可小觑，如其在俄罗斯的市场份额约为 30%。二是从资本层面控制他国互联网产业领域。中国电子商务 B2B 研究中心 2009 年 6 月发布的《中国互联网外资控制调查报告》指出，外资逐步从资本层面控制了中国互联网产业各个领域。特别是美国互联网资本几乎已经控制整个中国互联网产业。仅美国国际数据集团参与投资的中国互联网企业就有 20 余家，许多项目是中国互联网各个领域的领头羊，包括当当网、金蝶软件、携程网等。

美国历来重视通过经济途径传播价值观。美国凭借强大的国力，在多边和双边国际交往中将政治目的与经济援助和商业利益捆绑销售。对一个国家而言，一旦互联网市场被外资控制，要控制其中传播的内容，要掌握意识形态主动权，难度明显增大。更为重要的是，控制了互联网市场，就能攫取最为珍贵的资源——数据，也就掌握了一个国家各个领域的命门。美国深谙此道，不仅从技术、资金等方面助推本国互联网企业的发展和对外扩张，而且要求互联网企业与政府共享数据，其险恶用心昭然若揭。

（四）控制互联网信息主导权，利用网络资源优势对外进行文化输出，强化美国“文化霸权”

文化扩张是美国实现霸权的重要手段之一。互联网为美国“文化霸权”的扩张提供了一个全新的传播途径。美国牢牢掌控着互联网信息主导权，利用网络资源优势源源不断地进行文化输出，大力宣扬美国的文化和价值观念。目前，全球 80%以上的数据库集中在美

国；全球互联网的全部网页中 81%是英语；国际互联网上访问量最大的 100 个网站中，有 94 个在美国境内。网络空间在一定程度上可称为美国设计的文化环境，带有鲜明的美国文化烙印。

美国通过网络进行的文化扩张手段可视为“推”、“拉”结合。一方面，美国凭借强大的网络信息优势，利用其他国家对网络控制能力相对差和信息屏蔽能力相对有限的弱点，乘机将其价值观念、思维和生活方式，强制性地通过网络输送到这些国家。另一方面，美国依靠多彩的网络文化生活，增强其文化吸引力。好莱坞电影、迪斯尼动画和 MTV 等是其中的突出代表。美国通过语言、形象、明星和故事等元素使其文化产品潜移默化地将其文化理念及观念渗透给网络受众，使其他国家的民众尤其是广大青少年深受其影响。

无论采用何种方式，美国文化产品所宣扬的拜金主义、享乐主义和利己主义等价值理念都通过网络渗透到了全球政治、经济和社会生活的各个领域。这种文化渗透具有一定的隐蔽性，不会在短期内显露出来，却时刻影响着他国网络受众者尤其是青少年的思维模式和行为方式，从而逐步屏蔽其原有的价值观念，从根本上触及他国的民族传统文化、意识形态及价值观念。同时，美国网络文化霸权的推行又具有广泛性，包裹着美式“民主、自由、平等”的理念推行文化霸权，对他国进行文化颠覆。

（五）持续升级网络空间军事理念及战略实践，谋求美国在网络空间的战略威慑能力

美国既是互联网的缔造者，也是网络战的始作俑者。美国将网络安全上升到国家安全的高度，其对网络战争的重视也就不足为奇。美国近年来通过一系列动作，逐步完善了网络战争战略规划、军力建设等，并秘密进行了网络实战，引发了世界网络战军备竞赛。

美国十分重视对外网络战争战略和战术规则制定。美国防部先后发布了《国防战略报告》（2005 年）、《网络空间行动战略》（2011 年）和《网络空间战略》（2015 年），将网络空间作为与“陆、海、空、天”并列的“第五空间”，同时明确提出了网络震慑力量建设和主动出击战略。而在战术层面，则通过《塔林手册》、《网络空间联合作战条令》等，将网络攻击行为明朗化、规范化，完成了美国网络战争最贴近实战的一道“工序”。其次，美军探索形成了网络攻防战斗力生成的有效模式。2010 年，网络战司令部正式运行，使得美国网战力量进入统一协调发展的“快车道”；2012 年，为模拟真实网络攻防作战提供虚拟环境的美国国家网络靶场正式交付军方使用；2013 年，美国将网络司令部由 900 人猛增至近 5000 人，并宣布 3 年内扩建 40 支网络战部队。同时，为了加强其全球网络战力，美国积极结盟，将网络同盟作为发动网络战争的基本方式。近年来，美国邀请多国参加其发起的“网络风暴”系列演习，并不断扩大其邀请范围；同时，美国主要在北约范围内组织网络攻防演习，形成事实上的“网络北约”。从 2012 年开始，美国在北约范围内启动了“锁定盾牌”网络演习，旨在促进不同国家的国际协作，并逐渐将此演习变成其与盟国的网络练兵场。美国与传统军事同盟国家几乎都建立了网络军事同盟关系，多国联合作战极有可能成为美国发动网络战的基本模式。此外，美国还直接展开了网络实战，进行网络震慑。其中最为著名的非“震网”病毒破坏伊朗核设施莫属。2010 年 11 月，一种名为“震网”的计算机病毒对伊朗网络系统实施攻击，目标直指伊朗核设施，最终导致 1000 多台离心机瘫痪。由于这种病毒结构异常复杂、隐蔽性超强，专家普遍认为是由国家层面研发的。此后有美国媒体称美国曾和以色列共

同测试“震网”病毒，并认为美国是“震网”病毒的幕后老板。

三、美国千万百计向国际社会拓展“网络霸权”

为了推行网络霸权，美国将其阵线拓展到全球领域，通过主导互联网相关活动、鼓励国内公司和组织海外渗透、建立跨国互联网同盟等，将其触角伸向世界各地。在向国际社会推行其网络控制权方面，美国一方面高度重视与盟国的合作沟通，另一方面不遗余力地对发展中国家进行渗透，具有明显的战略层次性和区分度。

（一）加强与盟国之间在网络空间的战略合作，强化“网络战略联盟”关系

美国与部分发达国家在网络技术、网络安全和网络经济领域，通过双边和多边管道进行深度合作。如努力推动在欧洲安全与合作组织框架中实现“虚拟人权”，提升欧洲的“民主人权”和“网络自由”。美国的网络控制国际合作联盟中，以“五眼”（Five Eyes）情报联盟最为知名。该联盟由美国、英国、加拿大、澳大利亚和新西兰组成，将全球划分为五大监听区域，五国分别监听并共享资源，以实现在“任何时间、任何地点、（追踪）任何人”的目标。此外，新加坡、韩国、德国等也为美国进行全球监听出力不少。新加坡和韩国是美国主导的“五眼”间谍联盟在亚洲的伙伴国，在协助美国和澳大利亚在亚洲铺设海底通信电缆一事上立下“汗马功劳”。至此，已知的美国监听同盟遍布欧洲、亚洲、美洲、大洋洲等。而德国虽然一直刻画其美国监听受害者的形象，但德国情报部门也被踢爆是美国监听行动的“帮凶”，不仅曾帮助美国情报部门追踪本·拉登，甚至协助美国国家安全局对欧盟领导人实施政治间谍活动。

（二）利用互联网渗透扩展美国在“第三世界”的政治势力

在对待发展中国家方面，美国则通过经济社会援助和开展并主导网络项目的方式进行政治输出。美国务院组织“全球网络自由力量”，策划实施“公民社会 2.0”、“全球网络倡议”、“世界新闻自由日”、“网络治理论坛”、“网络自由跨区域声明”等多个国际活动，相关项目遍布世界各地，如 2011 年在智利、印度尼西亚、摩尔多瓦和乌拉圭等国先后举办了 4 次科技训练营，通过信息技术和政治传播能力训练，培训了来自至少 35 个国家的 250 个公民社会组织；在吉尔吉斯设立了“网络友谊车”，加强青年政治沟通；在斯洛伐克资助运行了“公平规则联盟信息项目”，推动政治公开；在中南美洲实施了“政治司法服务信息项目”，深度介入当地政治和司法进程。美国借助这些活动推行其“网络自由”战略，造成了较大的国际影响，获得了一定的国际支持。

（三）强化美国对硅谷企业及行业组织对外扩张的主导

事实上，美国在推行其网络控制权时，还积极借助其社会组织及公司等，鼓励国内公司和组织进行海外渗透。以谷歌、Facebook、推特等为代表的互联网企业代表美国政府立场和国家利益，扮演着美国网络霸权战略推行急先锋的角色。如推特等在中东政局震荡期间自愿沦为美国的传声筒，成为反对派信息传输的重要平台；赛门铁克、英特尔也使用美国的网络安全框架，甘愿为其服务。美国政府反复“敦促美国媒体公司主动采取措施”，“需要考虑什么是正确的，而不只是寻求短视的利润”。为最大限度地整合、利用企业力量，美国也做出

了多项努力。一是出台多项法律和行政命令如《网络技术共享和保护法》等，意在加强企业与美国政府的合作及信息开放共享。二是成立信息分享和分析组织如 ISAO，作为政府和企业的联系点。此外，以众多基金会如电子前哨基金会、新美国基金会等为代表的美国非政府组织也积极渗透到其他国家，为美国“网络自由”主张获取社会认可和舆论支持。例如，电子前哨基金会以推进全球网络普及和网络信息自由流通为己任，频频攻击别国信息管制，大力为美国推行网络自由战略造势。

美国军方网络安全战略解析

随着网络安全重要性的日渐增加，美国加强了对网络安全的管理，并力图完善美国网络安全的机制建设和战略规划。特别是随着“网络空间是美国五大核心领域之一”的国家战略确定并不断完善发展，美国军方也着手论证制定相关网络空间战略，制定和出台了一系列政策文件，并通过加大投资、扩编队伍、研发新技术等方式增强其在网络空间中的话语权。

一、确立网络战略框架

2004 年，美国参谋长联席会发布了《美国国家军事战略》，第一次将网络空间作为一个与陆、海、空和外太空并列的战斗领域。文件强调军事行动的三个重点：打击恐怖主义，增加联合作战，促进作战部队转型以应对未来全球挑战。

2006 年，参谋长联席会发布了《网络空间的国家军事战略》（NMS-CO）。这是美军第一份，也是迄今为止最为重要和权威的网络空间军事战略文件。该文件完整界定了网络空间领域，分析了在此领域的威胁和薄弱环节，并对未来态势进行了客观分析。其中专门讨论了网络安全问题。该文件指出了网络空间的特点、存在的威胁和脆弱性，并提出了一个确保美国在网络空间的军事优势的战略框架，包括六种手段和四个战略重点。该文件提出，国家网络空间军事战略的目标是确保美军在网络空间的优势地位。文件把网络空间的行动与国防部在军事、情报和商业领域的行为整合起来。

2011 年 7 月，国防部公布了《网络空间行动战略》，由于该战略绝大部分内容涉及军事机密，因此仅公开了小部分合计 13 页的内容。该战略的重点是通过规划美军在互联网领域的军事行动以确保美国的军事优势和维护战略资产安全。同时，还提出了五项战略措施：把网络空间视为与陆、海、空和太空同样重要的行动领域；运用新理念来保护国防部的网络和系统；加强与其他政府部门及民营机构的合作；加强与盟国及国际伙伴的合作；加强人才培养和技术创新。该战略发布后，有评论认为其“为国防部军事、情报和商业行动指出了新的前进方向”。

2015 年 4 月，美国国防部发布了新版《网络空间战略》。该战略是美国国防部对 2011 年 7 月公布的《网络空间行动战略》的进一步细化和落实。此次发布的网络安全战略虽仅为概要，但长达 33 页，内容明显比第一份战略更为详细和具体。之前美方主要强调了防御，几乎没有提及美军在网络空间的威慑和进攻能力，而本次战略明确提出要提高美军在网络空间的威慑和进攻能力。一旦遭受来自外界的网络攻击，美国的回应不会局限于网络回击，海陆空领域的常规军力打击也是必要选项。新战略细化了五大“战略目标”，同时为国防部在网络安全方面设定了三大任务：一是防卫国防部的网络、系统和信息；二是保卫美国国土及国家利益不受重大网络袭击活动的侵犯；三是集中网络军队力量支持军事行动和应急计划。新战略将中国、俄罗斯、伊朗和朝鲜列为对手。同时，将美国发起网络战的底线压低了很多，省略掉核查、确定网络攻击源等一系列过程，确定了美国国防部直接“开火”的权利。国防部发布的政策不需要再通过美国国会的批准，直接可以执行。

二、明确相关军种在网络战中的职能和任务

在网络空间国家战略和军事战略的指导下，美军各军种结合自身实际相继制定了各自的网络战能力发展规划。主要包括《空军网络司令部战略构想》、《2009—2013 年海军网络战司令部战略计划》和《陆军战略作战概念能力规划 2016—2028》三个战略文件。此外，美军各军种已开始着手网络战作战条令的制定。2010 年 7 月，美国空军已率先颁布了《空军网络战条令（AFDD3-12）》。该条令明确了网络战部队的指挥控制关系与职责、作战实施方法，并详细描述了空军网络战的设计、计划、实施和评估流程。这是迄今为止美军第一部正式的专门针对网络战而制定的作战条令。

三、采取多重措施提高网络战能力

美国的网络军事战略是一个综合性战略，其核心是提高部队的网络战能力，从而在未来数字空间的对抗中获得优势。美国希望通过全面发展自己在网络空间的行动能力，构建攻防兼备的网络战体系。为了提高网络战能力，美国在机构设立、研发资助、技术支持、队伍建设等方面采取了一系列的举措。

（一）机构设置方面

1. 设立网络司令部

2009 年 6 月，美国国防部部长罗伯特·盖茨正式发布命令建立美国“网络空间司令部”，以统一协调保障美军网络安全和开展网络战等军事行动。该司令部隶属于美国战略司令部，编制近千人，2010 年 5 月正式启动。司令部整合分散于各军种的网络战指挥机构，协调美军掌握的各种网络战武器，并制定运用这些武器的策略。此前，美军的网络管理权力分散，缺乏统一指挥。这次重组把美国网络司令部和国家安全局（NSA）安置在同一地点办公并且由一个人领导，从而最大限度地利用资源并提高决策效率。国家安全局既保障网络司令部的网络安全，又向其提供情报支持。此外，美军不同军种在网络空间的行动和信息也直接联系在一起。

2. 空军新成立编号网络航空队

2008 年年底，美组建空军网络司令部，总部设在路易斯安那州巴克斯代尔空军基地。2008 年 10 月，空军宣布第 23 航空队将作为空军航空司令部的一部分被赋予网络作战任务。2009 年 8 月，第 24 航空队正式成立。2010 年 1 月，美空军宣布第 24 航空队已初步具备网络作战能力，有超过 5400 名人员能支援或执行 24 小时的网络空间行动。作为空军对口的网络战指挥实体，第 24 航空队使空军成为最早完成网络战指挥机构整合的军种。其职能包括建立、扩展、维护和防御全球信息栅格的空军部分，作战进攻和为联合作战人员提供能力支持。目前，第 24 航空队隶属于空军航天司令部，下辖第 67 网络战连队（67NWW）、由空军信息站中心改编的第 688 信息战连队（688IOW，包括第 318 信息战大队和第 38 网络空间工程大队）、第 689 作战通信连队（689CCW，包括第 3、5 作战通信大队）、第 624 作战中心（624OC）和空军网络集成中心（AFNIC）。

3. 海军拓展网络战指挥机构职能

2002 年 3 月，美国海军率先成立海军网络司令部，成为掌控海军网络系统、协调情报技术、情报处理、空间需求和海军军事行动中心机构。2010 年 1 月 11 日，海军作战部长宣布在海军网络司令部（NNWC）的基础上，合并其他信息战、电子战等机构，正式成立舰队网络司令部（FLTCY-BERCOM）暨第 10 舰队（C10F），负责为海军全球范围内的网络空间、信息、计算机网络、电子和太空等领域的作战提供支持。每年网络防御经费高达 10 亿美元，司令部内组建了一支特殊队伍——海军红色战队，该分队中有 34 个精通密码技术的网络工程师和 7 个技术高超的黑客。舰队网络司令部职能比其他同类型司令部复杂，其主要作战力量即第 10 舰队采用了非常典型的海军特遣部队编制结构。其中，NNWC 作为网络特遣部队 1010（CTF1010）负责网络运行，其下属部队包括海军大西洋计算机与电信区域主站（NCTAMS）和太平洋 NCTAMS，为舰队提供网络连接、维护和岸上中继；海军网络防御作战司令部作为 CTF1020，负责网络威胁探测和安防响应；信息战任务则由诺福克海军信息战司令部（NIOC）（CTF1030）负责，下辖圣地亚哥和韦德贝岛的两个分队；舰队和战场作战及密码业务则由佐治亚 NIOC（CTF1050）、马里兰 NIOC（CTF1060）和科罗拉多 NIOC（CTF1080）及其全球分布的下属司令部分属司令部分别负责协调；此外，海军休特兰信息战中心（CTF1090，Suitland）被指定为专门的研发机构。此前舰队网络司令部所属编制人数已达 44000 人。

4. 陆军明确网络战职能机构及分工

2001 年，美陆军司令部开始筹划建立计算机网络战办公室，建立了计算机应急响应分队。2010 年 10 月 1 日，陆军正式成立了陆军部队网络司令部，作为独立指挥机构统一领导陆军网络空间领域内的所有任务。该司令部的主要职责是配合网络司令部组织、训练和装备网络部队，确定陆军任务需求和部队能力；在得到网络司令部的指令时，其还将为组建联合特遣部队提供支持；此外，该司令部还负责 DoD 信息网络陆军部分的态势感知，支持网络空间作战，以使网络司令部司令能使用统一的联合网络空间作战视图，实施高效作战指挥控制。其主要下属机构包括陆军网络企业技术司令部（NETCOM）、情报与安全司令部（INSCOM）和拟建的陆军网络作战和集成中心（ACOIC）。陆军部队网络司令部成立后，所属编制力量由 NETCOM/9thSC（A）目前下属人员、第 1 信息战司令部和 USASMDC/ARSTRAT 的一部分，以及 INSCOM 下属网络作战人员构成，总人数达 21000 人。

（二）能力建设方面

1. 研发网络防御装备

美军网络防御技术研究领域通常将网络防御能力分为信息环境保护、攻击探测与恢复三种。为实现这些能力目标，美军的网络防御采取国防部深度防御策略。要求综合利用人员、技术和操作能力，在技术层面上建立从网络基础设施、飞地边界到计算环境的多维、多层防御，并加强密钥管理暨公钥基础设施、检测与响应基础设施的建设。此外，美军还非常重视“主动网络防御”概念的应用，即通过一定的技术手段，找到攻击源，并予以实时还击，达到威慑目的。依据主动、深度防御策略，美国防部专门制定了“信息保障和生存能力计划”。该计划包括战略入侵评估计划、入侵容忍系统、故障容忍网络、信息保障科学工程计划、网

络空间指挥控制战计划等 8 个子计划。美军还投入了数百亿美元用于研制开发各种网络防御系统和技术装备。最具代表性的装备包括“网络诱骗”系统、“网络狼”软件系统、网络攻击报警系统和网络漏洞扫描仪等。

2. 研发网络进攻装备

美军的网络进攻技术研究以网络欺骗能力以及破坏或摧毁敌方网络技术为重点。其中，网络欺骗技术通过分析信息的格式和长度等属性，对其内容进行篡改，以实现欺骗对方的目的。而在破坏与摧毁技术方面，美军的蠕虫、特洛伊木马程序、逻辑炸弹和计算机病毒等恶性代码破坏、瘫痪网络的能力正在增强；拒绝服务攻击方式可利用成千上万的计算机向一个网站发送信息，使其服务中断，可用于攻击军用信息网和战术无线网等目标；另外，美军开发的网络攻击技术还包括硬件“隐藏雷”攻击技术、后门攻击技术、重放攻击技术、信令攻击技术和网管攻击技术等。美军开发的最具代表性的网络攻击装备是“舒特”系统。美军的“舒特”系统是网电一体作战的典型手段，已从“舒特 1”发展到“舒特 5”，作战效能不断提升。“舒特”系统以电子干扰电磁波、敌方防空雷达探测电磁波等为载体实施入侵攻击，取得系统控制权限后，通过修改作战参数，或者利用“木马”病毒瘫痪敌方防空雷达系统，达到突袭目的。

此前，有媒体援引斯诺登文件称，美国国家安全局正在进行一项名为 Politerealin 的计划，该计划由国家安全局“获取特定情报行动办公室（TAO）”执行，主要内容是入侵特定的计算机并进行破坏性活动。Politerealin 计划的目的是使计算机网络系统瘫痪以便于进行远程控制，覆盖面包括能源供给、水利系统、工厂、机场和金融系统。个人用户方面，几乎所有防火墙都可被入侵，社交网络 Facebook 聊天内容及手机用户信息也可被复制。

3. 研发网络侦察装备

在网络战实施过程中，利用或摧毁敌方网络的行动必须以探测、跟踪和定位敌方雷达、微波站、蜂窝电话、卫星地面站和其他通信链接等设施为前提。美军认为，只有对战场信息流进行有效控制（如侦听移动电话和截获电子邮件），才能掌握未来网络对抗的主动权。为此，美军近年来加强了网络侦察技术的研究。目前，美军在无线监听、搭线监听、口令破解、网络分析等技术上已取得较大进展，具备获取敌方通信、内容、网络协议、硬件地址、口令、身份鉴别过程、网络漏洞等信息的能力。目前，美军最具代表性的网络侦察装备包括“高级侦察员”网络侦察系统、“分析、传播、直观化、深入理解和语言强化（ADVISE）”系统和“网络中心协同定位（NCCT）”系统等。

（三）资金投入方面

在美国国防预算持续削减的背景下，美国国防部仍加大在网络部队和网络武器方面的投资表明了美军对网络空间军事化的重视。美国国防部用于网络安全技术研发与人员培训的年均投入达 30 亿美元。截至目前，美军已先后投入了数百亿美元用于研制开发各种网络防御系统和技术装备。2011 年，美国国防部曾决定在未来 5 年内拨款 5 亿美元给国防部高级研究项目局，以加快网络武器及防御性网络技术的研发。2013 年 5 月，美国国防部与数据策略公司签署了约 2580 万美元的合同，并与雷神公司签署了约 975 万美元的合同。这些公司负责开发用于网络战的设备和软件。鉴于此前美国国防部已经开发过大量用于网络战的设备

和病毒软件，未来的网络武器将更注重性能的提升，某些新式网络武器甚至可以帮助美军在敌军军事系统未接入互联网的情况下对该系统实施攻击。此外，提高自我修复和入侵忍耐能力对维护有弹性的网络意义重大。考虑到国防部运行 1.5 万个网络，涉及 700 万个设备，成功实施高级技术（自我修复、入侵耐受）是个巨大的挑战。要执行这些技术，需要更换设备、软件和互联网协议。2014 财年，国防部建议网络行动方面的预算为 47 亿美元，比上一财年增长了 21%。

（四）网络队伍建设方面

通过加强网络部队建设，美国的网络战能力在不断提高。美军网络司令部一开始编制只有 900 人，但 2013 年有报道称将扩编至 4900 人。2014 年 3 月 28 日，美国国防部部长哈格尔宣布到 2016 年将网络司令部在编人数扩至 6000 人。而美军网络司令部司令罗杰斯在 2014 年 9 月的比林顿网络安全会议上透露，网络部队人数将在 2016 年前增至 6200 人。2015 年 4 月发布的新战略将美国网络军队司令部的直属队伍进行了调整，由原计划的 140 个改为 133 个，区分上也有了变化，多了 13 个“国家任务力量”队伍和 27 个先前未曾提及的“战斗任务力量”队伍。

美国网军由 3 个分支组成，除保护美国国内电网、核电站等重要基础设施的网络部队外，还有协助海外部队策划并执行网络袭击的“进攻性”部队，以及保护国防部内部网络的“防卫性”部队。前者已于 2013 年 9 月投入运行，后两个分支也将在 2015 年组建完成。斯诺登的文件显示，约有 4 万名员工参与监听和网络攻击及反攻击工作。

1. 人员招募

为了充实网络战后备军并保持网络人才优势，美国国防部每年都从全美各大院校招募大量计算机、数学、语言学等专业的优秀毕业生。此外，国防部通过与总统执行办公室合作，设立动态的规划来吸引人才，具体措施包括：简化录用程序、人才“无害流动”、开发预备役和国民警卫队的网络能力、继续教育等。

2. 人员资质要求

美国防部规定，处理国防部信息业务的人员，必须具有上岗资格证书；应聘到国防部门从事信息安全工作的人员，要具备相应的专业证书。再版 DoD 第 8570 号指令规定，所有军方、联邦政府、外事单位聘用的全职和兼职文职人员都必须依照工作内容通过安全资格认证计划（SCP）的 SCNS、SCNP 及 SCNA 三类安全资格认证考试，相关人员在 2010 年必须通过该认证。

3. 人员培训

依托院校和卓越训练中心等机构，美军为网络战部队开设了大量网络基础课程。既有针对某一军种或某一业务特定需求的专门课程，如“陆军计算机网络作战规划者基础课程”、“联合网络分析课程”和“联合网络进攻课程”等，也有满足联合网络空间训练需求的通用课程，如国家安全局设计的“跨学科网络课程”等。同时鉴于各自对网络空间训练的不同需求，自开始大规模组建网络部队以来，各军种都相继展开全面评估，以确定不同的基本训练需求。

4. 后备人才库培养

近年来，美国国家安全局在“网络行动计划”（COP）下设立了“国家优秀学术中心”（CAE）项目。该项目通过在一些特定大学开设与网络攻防技术有关的课程，普及有关网络战的知识。据报道，国家优秀学术中心开设的课程除了普通的计算机编程、网络维护外，还包括编写计算机病毒、入侵网络、破解密码、数据挖掘等。2012 年 5 月，国家安全局宣布四所大学获准参加“国家优秀学术中心”项目，分别是达科他州立大学、海军研究生院、东北大学和塔尔萨大学。2013 年 9 月，国家安全局宣布又有四所大学参与这项计划，它们是空军技术研究院、奥本大学、卡内基 • 梅隆大学和密西西比州立大学。

5. 举行实战演习

近年来，作为检验网络作战部队训练效果、提升作战能力、试验网络武器效能、验证作战理论的重要举措，美军定期举行网络战实战演习。美军内部组织或参与政府组织的专门网络战演习包括“联合远征部队实验”、“数字珍珠港”、“黑色恶魔”、“寂静地平线”和“网络风暴”系列演习等，有众多国家和机构参与，规模庞大、投入高、针对性强。此外，美军还非常重视在规模不一的各种联合演习中设置网络攻防科目。如在每年的“焦点透镜”和“阿尔索伊 / 鸽鹰”联合演习中均设有网络攻防科目，根据联合作战整体意图和战略战役目的，演练网络战在信息化条件下一体化、联合协同作战行动。此外，美国和韩国于 2010 年 7 月 25 日至 29 日在日本海举行的“不屈意志”联合军演中，网络防御作战就是重要演练内容之一。

6. 建设模拟训练设施

美军还非常重视网络对抗训练模拟系统的建设，将其作为网络对抗技术学习、研究和训练的重要平台。其主要功能包括：模拟网络攻击的各个主要步骤，实现目标侦测、信息窃取、网络入侵、信息或服务破坏等攻击方法；观察和检测各种网络攻击行为，正确评估攻击效果；通过采取有效防护措施控制安全风险，并根据防御训练后的评测结果比较攻防效果；提高参训人员的信息安全意识，增强网络对抗的实践技能。同时，美军正着手模拟训练基地的建设，如空军已将尼尔森空军基地作为网络战战术、技术和实施的训练场地。此外，DARPA 建设中的“国家网络靶场”，除主要作为网络攻防手段测试设施外，也能为网络攻防作战提供虚拟环境，还是提高训练水平的重要基础设施。

美国国防部 2015 年新版网络战略述评

美国国防部于 2015 年 4 月 23 日发布了《美国国防部网络战略 2015》，这是对 2011 年 7 月发布的国防部《网络空间行动战略》的升级，为国防部未来五年的网络活动和任务设定了优先实现的战略目标。新战略明确了三大任务：一是保护国防部的网络、系统和信息；二是保卫美国国土及国家利益不受重大网络袭击活动的侵犯；三是集中网络军事力量支持军事行动和应急计划。新战略提出了五大目标：建立和维持网络力量和能力以进行网络空间作战；保护国防部信息网络、确保国防部数据安全和减轻国防部任务风险；保护美国本土和美国切身利益免受具有严重后果的破坏性网络攻击；建立和维护可行的网络方案并在各阶段控制冲突升级以及营造有利的冲突环境；建立和维护强大的国际联盟以阻止威胁蔓延并增强国际安全与稳定。

一、相比 2011 年版网络安全战略的新特点

（一）态势分析

面临的网络威胁更严重。美国国防部发布的网络战略情况说明显示，促使国防部制定新战略的重要原因是美国政府和企业遭受网络攻击的紧迫性和复杂性不断增加。新战略强调恶意软件泛滥以及“危险和不可控”的网络漏洞的风险，而 2011 年版战略则认为国防部可以阻击绝大部分的网络漏洞和恶意行为。值得注意的是，新战略称中国、俄罗斯和伊朗的黑客是攻击美国网络的主力，这是奥巴马政府在 4 个月内第 4 次点名涉嫌黑客攻击的国家。

（二）架构设计

更突出和强调军方的作用。2011 年版战略提出加强公私合作、与国土安全部之间的合作，新战略则直接将“保障本土和核心利益不受破坏性网络攻击”等写入国防部的任务，民营机构运营的网络基础设施也被纳入国防部保护。新战略将网络空间作为新的作战领域，扩大在网络空间的军事能力，增加在网络空间的军事选项。这将对美国网军司令部的职能、结构和建设计划产生深刻的影响。新战略将美国网络军队司令部的直属队伍调整为 133 个，增加了 13 个“国家任务力量”队伍和 27 个以前未曾提出的“战斗任务力量”队伍。同时，新战略更加细化，详述了国防部在网络战中的作用及如何整合网络能力。

（三）指导思想

更强调先发制人和进攻性。美联社分析文章认为，2011 年版战略强调防御，几乎没有提及军方的网络攻击能力。而新战略中攻击性明显提升，强调报复能力。新战略称，“总统或国防部长可决定让美军开展网络行动，以扰乱对手与军事相关的网络或基础设施，让美军能够在开展行动的区域保护美国利益”，“国防部应能用网络操作来扰乱敌人并控制网络，破坏与军事有关的重要基础设施和武器功能”。这为先发制人地开展网络攻击留下了空间。

（四）制度设计

更强调与相关法令的配合。2011 年版战略只在与国土安全部的合作中提到了有关的法律约束，而新战略在法律方面有全面升级。新战略指出，国防部在网络空间的活动要受美国国内法和相关国际法的双重约束，比如提到了《武装冲突法》的相关适用情形。在新战略发布的同时，近期美参众两院还分别通过了《网络安全法案》、《网络空间安全信息共享法》、奥巴马总统网络攻击制裁令以及《网络安全保护法案》。在过去几年，美众议院表决相关法案时曾多次受挫，但近期索尼影业等黑客攻击事件扭转了形势。分析人士称，这些法案为美国发动网络攻击提供了法律依据。

（五）首次将中、俄等国明确为潜在威胁

新战略明确提出了网络空间的潜在敌人：俄罗斯、中国、伊朗、朝鲜及“伊斯兰国”等。虽然美国一直有个假想敌名单，但 2011 年版战略中只笼统地提到网络空间的对手，没有直接点名，新战略却将中国、俄罗斯、伊朗和朝鲜等国家作为对手提出来。有分析指出，从新战略可以看到这种可能性：如果将来中国在南海、钓鱼岛有所行动的话，美国可对中国的关键设施实施网络攻击。

二、新战略中几点值得注意的趋势

（一）整合多种网络力量，加快技术研发和创新

美国防部称，将集成网络能力，支持军事行动和应急预案。如军方和网络司令部在网络战中有不同的职责。国际战略研究中心战略技术项目高级研究员丹尼斯·郑表示，目前各军种有自己的网络平台，系统冗余并且需求不一致。新战略计划统一网络作战平台，并与国土安全部、国民警卫队、执法部门、情报部门及其他政府机构进行合作。国防部将改善网络作战的指挥技术、相关工具及预测分析能力，同时加快基础研发和应用以实现网络技术的跨越式发展。

（二）推动军民融合和线上线下能力的整合

新战略突破了传统的网络战略“军民两分”的规则，提出了“加强政府部门以及公私机构的网络安全信息共享”、“与教育机构、民营部门和企业合作”。国防部部长卡特表示将与硅谷合作，吸引产业界和学术界的优秀人才从事网络相关研究开发。新战略突破了常见安全战略手段中“线上线下两分”的规则，要求美国网军司令部、参谋长联席会议及国防部部长办公室协调运作。新战略中频繁出现“全频谱”、“结合威慑”以及“积极防御”等概念，可见美国已逐渐将网络攻击与常规军事力量相结合。新战略还突破了传统战略聚焦系统、基础设施、软硬件的特点，将数据升到了系统安全的高度，提出了“保卫国防部网络和数据”、“各机构必须仔细确定需要优先保护的系统和数据”、“帮助盟友建立保卫网络和数据的能力”等。

（三）强调新网络攻击层级体系的构建

新战略首次明确表示，美军在与敌人发生冲突时可考虑实施网络战。与此同时，作为新战略的核心内容，还进一步明确了网络攻击的层级体系：公司和民营机构负责抵御常规攻击，

美国国土安全部负责检测更复杂的攻击，并帮助民营部门实施防御。美国防部官员表示，美国网络系统遭受的攻击中，约 2%可能上升到国家级响应，即由五角大楼牵头，通过马里兰州的国家安全局的网络司令部回应。

（四）重视国家网络能力的建设

新战略重视依靠国际联盟和伙伴关系阻击网络攻击，提出加强与网络攻击相关的情报收集能力，特别提到了在中东、亚太地区和北约共同开展相关工作。对此，有美国媒体认为，国防部应该对网络空间中的军事理论、政策、角色和任务有更为清晰的阐述，以便更好地让公众知晓，并进行相关的宣传和讨论。

三、可能带来的影响分析

（一）引发网络军事化及网络军备竞赛

新战略是美国新国家安全战略的具体落实，预计美国还将推出相关政策和立法，以获得单边的网络安全并保持网络空间的领导地位。新战略在网络空间非军事化上是重大退步，美国放弃网络空间非军事化的立场，将令国际社会维持网络和平的期待受挫。美国网络司令部的设立是网络空间军事化最典型的例子。受美国先发制人策略的刺激，不少国家都可能推进网络空间军事化。先发制人需要建立优势，而这可能引起新的军备竞赛。大国考虑攻击性网络武器，小国由于在传统武器上没有优势而更加热衷于发展网络武器。美国先发制人的战略极易溢出到其他领域，演变成诱发全面冲突的“危险性游戏”。

（二）中美网络安全领域“对话和对抗交织”将成常态化

新战略首次提出，美国对于中、俄等国针对美国“持续不断的网络间谍活动”给予关注，将促进了解以减少误解和错判的风险。但是联系近期中美两国相互限制采购对方的信息技术系统、中国出台《国家安全法》规范网络安全审查等事件，《纽约时报》评论称中美已进入“网络冷战”。近期，习近平主席访俄期间中俄两国签署了网络安全合作协议，很多美国媒体认为此举针对美国。

（三）网络冲突可能成为现实战争的导火索

从 2011 年的《网络空间行动战略》到 2013 年的《塔林手册》，再到新网络安全战略，美国将现实武装打击作为应对网络攻击的手段。由于技术所限，网络攻击较难追溯，美国的网络攻击指责缺乏直接证据，甚至需要通过网络攻击来确认对方是否攻击。这种情况下，可能出现美国以网络攻击为借口武装入侵他国的现象。网络冲突已成为全球安全最广泛的破坏因素。

四、对我国的启示

（一）加快制定网络安全战略，做好网络基础设施防护工作

我国应形成清晰的网络空间战略框架，完善国家网络战略布局和顶层设计。针对网络空

间关键领域统筹制定行动计划，建立完善的网络安全保障体系。应尽快出台网络安全战略，在继续确保互联网内容和意识形态安全的同时，要对网络基础设施等的安全问题给予高度重视，确保以基础设施安全为核心的综合性网络安全。此外，随着美国网络情报刺探持续升温，对华网络基础设施的刺探也持续提升，我国要做好网络基础设施遭遇美国攻击的准备。

（二）加强网络安全领域的军民融合

网络安全自主可控产业应纳入国防工业体系，为网络国防提供战略支撑。自主创新是网络国防的必由之路。应加强核心硬件、基础软件和关键技术的研究，加强军民融合和行业联盟，合力攻坚，提高关键技术的自主可控水平。以开放、合作的心态吸收先进理念和技术，充分利用企业的技术、人才和市场优势，采取政策引导积极拓展企业参与网络国防建设的渠道。

（三）围绕网络安全构建系统的法律制度

美国国会、联邦政府和最高法院通过发布立法、行政命令及判例的方式，构筑起网络安全治理的完整法律体系。该体系既明确了权力，也对权力运行的程序与边界等作了严格的规定。我国网络立法仍然严重不足，立法层次较低，体系分散，在具体制度的科学性、合理化、完整度等方面也存在明显的欠缺。有必要加强网络空间立法研究，建立国家网络安全法律体系。

（四）加强网络安全国际合作

美国新战略将产生新的网络安全的合作机遇。我国应积极参与政府间网络安全合作，加强与俄罗斯、美国、欧盟等国家和地区间的对话，形成重大网络安全事故沟通和协调机制。明确公开我国对网络战争的立场，强调各国有责任保护本国网络空间免受威胁、干扰和攻击破坏。

浅析近年来美国网络安全立法的焦点及争议

进入互联网时代以来，网络安全问题及其对经济发展、国家安全和社会稳定的重大影响日益凸显。在信息网络化进程中，国家安全与经济、政治的安全日益不可分割，而经济、政治安全越来越依赖于关键性信息网络基础设施的安全。网络安全是一个事关国家公共安全的全球性重大战略问题，已成为世界各国政府的共识。美国作为全球网络技术的发源地，掌握着网络空间的核心技术，在网络安全领域的立法也起步最早，数量最多，覆盖面最广，内容最复杂。可以说，在网络空间安全立法方面，美国一直处于世界领先地位。

近年来，随着威胁国家安全的恐怖袭击和网络监控事件频繁曝光，美国国会出于对国家利益的考虑更是加快了网络安全的立法进程。然而，虽然参众两院提出了众多立法提案，但始终面临复杂的阻力和争议，立法进程艰难，最终成文的法律成果寥寥可数。但国会始终积极推进，且目标明确，脉络清晰。了解美国近年来立法进程的焦点和阻力，将为我国建立网络安全法律保障体系提供有益借鉴。

一、美国网络安全框架性法律

据美国国会研究部统计，从 1984 年至 2009 年，美国通过成法、含有网络安全相关条文的法律有 36 部。其中一些框架性法律对网络安全的关键问题作出了重要规定，是美国网络安全法律体系的基础，见表 1.2。

表 1.2　美国主要的网络安全法律及内容

时间	法律文件名	内容简介
1984 年	《伪造接入设备及计算机欺诈与滥用法》	禁止对联邦政府的计算机系统、银行以及在州际、国际贸易活动中所使用的计算机系统进行各种攻击
1986 年	《电子通讯隐私法》	禁止未经授权的电子窃听
1987 年	《计算机安全法》	规定美国国家标准与技术研究所负责为联邦政府的计算机系统（用于国防和情报任务的国家安全系统除外）制定安全标准，商务部部长负责安全标准的公布
1995 年	《缩减文书法》	授权联邦政府行政管理和预算办公室（OMB）负责制定网络安全政策
1996 年	《信息技术管理改革法》	美国政府部门长官负责制定本部门的信息安全政策和规程，并在各政府部门设立“首席信息官”职务
2002 年	《网络安全研究与发展法》	美国国家科学基金会和美国国家标准与技术研究所在网络安全研究方面负有责任
2002 年	《电子政府法》	从法律上指导联邦政府开展信息技术管理和行动，保障网上信息与服务，提出相关网络安全要求
2002 年	《国土安全法》	赋予国土安全部部分网络安全职责
2002 年	《联邦信息安全管理法》	明确并加强美国国家标准与技术研究所和联邦机构的网络安全方面的责任，建立统一的联邦突发事件响应中心，让联邦政府行政管理和预算办公室而不是商务部部长负责颁布联邦政府的网络安全标准

从内容上看，以上框架性法律从保护网络基础设施、网络泄密与数据保密、打击恐怖主义和网络色情活动等多个方面确立了互联网行为的基本原则，初步建立起多维度的法律保障体系。进入 21 世纪，为应对互联网的飞速发展和国际形势的风云变幻，美国已开始着手网络空间的顶层设计，2011 年相继发布了《网络空间国际战略》和《网络空间行动战略》，并把网络空间作为与“陆、海、空、太空”并列的美军“行动领域”，网络战略突出“主动防御”，“保留”以军事打击回应网络攻击的权利。为了配合国家战略，不断完善和加强网络安全法律框架显得日益紧迫。

二、第 112 届国会以来的立法进程及关注焦点

（一）近年来网络安全立法进程艰难

自 2002 年以来，除了一些对已有法律的修正案，并没有通过任何重要的网络安全立法。尤其是第 112 届国会以来（2011 年后），虽然众议院、参议院和白宫都提出了数量庞大的网络安全议案，涉及网络安全的诸多方面，既有综合性的网络安全法案，也有就网络安全的某个具体问题而提出的法案，但是由于多方利益、意见分歧，这些法案在一次又一次的修订后，仍很难获得通过，成为正式法律文件。

美国第 112 届国会和第 113 届国会关于网络安全的主要立法建议如下。

1.《2012 年网络安全法案》（Cybersecurity Act of 2012）

2011 年以来，参议院一直试图将第 111 届国会期间国土安全和政府事务委员会提出的 S.3480 号法案和商务、科学和运输委员会提出的 S.773 号法案合并成一部综合性的网络安全法律。2012 年 2 月，参议院提出吸收了上述两个法案主要内容的《2012 年网络安全法案》（S.2105），随后又提出了该法案的修正版本（S.3414）和替代版本（S.3342）。《2012 年网络安全法案》获得了美国总统、政界、军界和情报界的大力支持。但这些法案在第 112 届国会均未获通过。

《2012 年网络安全法案》的主要内容有：一是加强对关键基础设施网络信息安全威胁的研判，成立专门机构，加强对关键基础设施网络的风险评估，完善风险信息的互动机制；二是重视公私合作应对网络安全风险，发挥关键基础设施运营部门积极性，听取其关于开展安全实践行动的建议；三是鼓励民营部门自主开展网络安全行动，政府协助创造良好的环境，确保参与者的相关利益；四是促进信息共享，建立公私间共享网络安全相关信息的框架，同时重申保护隐私和自由权利的原则；五是提升政府网络安全水平。此外，《2012 年网络安全法案》还对美国联邦网络安全人才管理、信息安全技术研发管理等作出了规定。

2.《2012 年确保IT安全法案》（SECRUE IT Act[1]）

2012 年 3 月参议院以 S.2151 号法案首次提出《2012 年确保 IT 安全法案》，后提出修正版本 S.3342 号法案。2012 年 7 月，S.3342 号法案进入议会辩论，但未通过 8 月 2 日的撤案动议投票，在 11 月 14 日的投票中再次失败。

[1] SECURE IT 全称为 Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology。

《2012 年确保 IT 安全法案》主要内容有：一是授权民营企业采取对策，使用网络安全系统来获取、识别或掌握其网络上的威胁信息，具备此类授权的企业也可以获取、识别或掌握其他企业的网络威胁信息；二是允许民营企业，非联邦政府机构，或州、部落及地方政府向指定网络安全中心或彼此之间主动披露网络威胁信息，以协助阻止、调查或减少安全威胁。

3. 众议院的 4 项网络安全立法提案

2011 年 10 月，众议院共和党网络安全任务小组发布了一系列立法建议，共发起 6 项立法提案。2012 年 4 月 23 日，其中 4 项提案通过众议院投票，但最终未被纳入参议院的议程中。

- 《2011 年网络安全强化法案》（H.R.2096），对美国联邦网络安全研发作出规定，并完善了技术标准，作为 H.R.756 议案在第 113 届国会被再次提出。
- 《2011 年网络情报共享和保护法案》（H.R.3523），主要对信息共享与协作作出规定，包括机密信息共享。在第 113 届国会中该法案作为 H.R.624 议案被再次提出。
- 《2012 年推进美国网络信息和技术研究及发展法案》（H.R.3834），主要对网络与信息技术研发作出规定，包括但不限于安全领域。
- 《2012 年联邦信息安全修改法案》（H.R.4257），主要关于《联邦信息安全管理法》的修改方案。

2013 年参议院和众议院提出但未成法的网络安全法案见表 1.3。

表 1.3　2013 年参议院和众议院提出但未成法的网络安全法案

议案号	议案名称	提出日期（2013 年）
参议院		
S.21	《网络安全及美国网络竞争力法案》	1 月 22 日
S.658	《2013 年网络勇士法案》	3 月 22 日
S.884	《阻止网络盗窃法案》	5 月 7 日
S.1111	《网络经济间谍责任法案》	6 月 6 日
众议院		
H.R.86	《网络安全教育加强法案》	1 月 3 日
H.R.624	《网络情报共享和保护法案》	2 月 13 日
H.R.756	《网络安全研发法案》	2 月 15 日
H.R.967	《2013 年推进美国网络和信息技术研发法案》	3 月 14 日
H.R.1121	《2013 年网络隐私强化法案》	3 月 14 日
H.R.1163	《2013 年联邦信息安全修正法案》	3 月 14 日
H.R.2281	《网络经济间谍责任法案》	6 月 6 日

（二）六大网络安全立法焦点

虽然立法建议进展艰难，但近几届美国国会仍不断修正立法提案，努力推进网络安全立法，立法方向主要是保护关键性基础设施以及促进政府与产业界之间的信息共享。归纳以上未能通过的法案内容可以看出，美国近年来的网络安全立法旨在推动解决以下六个方面的重点问题。

1. 保护私有关键性基础设施

2012 年 7 月，美国国家安全局局长基思 • 亚历山大在一个安全论坛上称，“自 2009 年以来，针对基础设施的网络攻击数量增长了 1700%。”美国联邦政府确定了 16 个领域的关键性基础设施，即核心制造业、核工业、化工业、国防基础工业、能源业、运输业、金融服务业、信息技术、通信设施、政府设施、商务设施、医疗和公共健康、急救、食品和农业、水资源和废水处理、水坝。这些领域的网络安全对国家安全至关重要，而绝大多数关键基础设施为私有，美国政府不可能强行将其纳入监测防御系统，只能谋求其他解决方案。政府不断试图通过法律手段保护关键基础设施的安全。

2. 促进部门内部及公私部门之间的信息共享

联邦政府认为，为有效保护信息系统，应减少或清除有关部门内部及部门间的信息共享壁垒。这包括明确信息共享的主体，规定如何共享某些机密信息，规定如何与民营部门进行信息交换，限定政府部门将共享信息用于特定目的等。

3. 培养网络安全专业人才队伍

建议措施包括增大联邦政府网络安全专业人员规模，加强对“下一代”网络安全专业人员的培训，实现联邦与民营部门专业人员交流，建立网络安全人才管理体系等。

4. 修订《2002 年联邦信息安全管理法》

该法自通过之日起就因存在诸多漏洞而饱受批评，包括：法律规定的网络安全标准未被广泛认可，对联邦机构相关授权的解释含混不清，过于强调个人信息系统而忽视了整个联邦信息系统，过于强调程序性的报告制度，可操作性不强，对加强联邦机构间协作缺乏明确的规定等。

5. 注重网络安全技术的研究与开发

《2002 年国土安全法》没有提及网络安全研发问题，但实际上国土安全部、国家安全局及其他一些联邦机构在网络安全研发方面投入了大量资金。因此，联邦政府急需相关法律以进一步明确涉及网络威胁和侵入的侦测设备、身份管理、各种测试设备以及电子设备全球供应链安全的研发究竟由哪个部门负责。

6. 授权指定政府部门负责网络安全

国会的相关法案主张增加对国土安全部在保护联邦信息系统方面的授权。

部分法案和白宫建议还关注了数据泄露通知和惩治网络犯罪的问题。

三、网络安全立法面临的争议和阻力

美国联邦政府在解决网络安全问题方面面临诸多挑战，因为一方面涉及保护联邦政府信息系统的安全，另一方面也涉及在保护非联邦政府信息系统方面联邦政府如何发挥适当的作用。目前美国各界对于国会立法的政府过度干预、增加运营成本、隐私信息泄露等问题争议不断，利益难以达成一致，这是近年来立法提案频频失败的主要原因。

第一，增加了政府对民营企业的干预程度，也提高了企业运营成本。美国商业团体认为，网络安全法案的诸多安全要求同企业的核心业务和操作密切相关，尽管法案明确表示企业的

网络安全实践基于自愿原则，但这对企业而言仍然是一项非常烦琐且花费巨大的工程。共和党批评者认为，法案的网络安全实践，无论是强制性还是自愿性的，都将使私人企业陷入资金链紧张的境地，政府没有必要在这一问题上进行干预。

第二，担心政府侵犯公民隐私权。美国部分专家认为，部分法案赋予了政府网络全控权。如果说针对电力网络、供水系统等关键基础设施的网络安全与国家安全息息相关，那么情报部门针对 Facebook 和 Twitter 等应用用户的监控则显得没有必要，还严重侵犯了公民隐私权。例如，《2012 年网络安全法案》赋予民营企业监视用户的权力、与政府机关共享信息的权力以及针对上述行为的法律豁免权，就引起了巨大争议。众议院 2012 年通过的《网络情报共享和保护法案》也致力于促进政府和企业之间的信息共享，但是该法案受到了工业界、隐私保护团体的阻碍。

第三，认为网络安全法案未能广泛听取各方意见。随着互联网日益发展，网络安全的利益相关方日益增多，涉及政治、经济、文化、外交、军事、科技等多个行业和部门。如何平衡多方利益成为一大难题。部分法案由于未能听取广泛意见而遭到国会相关利益代表反对。反对者认为，网络安全法案的推动者应该具有更广泛的视角，应开展与商业团体、网络安全研究人员和网络犯罪法律专家等各界人士的对话，而不是只听取既得利益团体的建议。

第四，民营企业认为自身可以达到网络安全目标。美国商业团体认为，目前由国际标准化组织（ISO）等制定的网络安全标准和较成熟的网络安全解决方案众多，民营企业完全有能力做好网络安全防护工作，而政府监管只会造成阻碍。目前 ISO 已制定了 189 项信息安全相关标准，美国国家标准与技术研究所（NIST）也已经制定出一整套世界级的信息安全指导资料和标准，民营企业倾向于依靠自身力量实现网络安全目标。

第五，国土安全部的授权程度尚未明确。《2002 年国土安全法》授予国土安全部部分网络安全职能，美国国土安全信息网络允许各州、主要都市地区在联邦、州和地方机构之间收集和分发信息，共同打击恐怖主义。但国会对于国土安全部在保护联邦网络信息系统方面的授权程度问题上意见不一。

四、美国网络安全立法进程对我国的借鉴意义

虽然近年来美国网络安全立法面临重重困难和各方争议，但国会立法进程不断加速，立法提案更有针对性，覆盖领域更加广泛，推进力度也日益加强，足见网络安全作为国家安全重要组成部分的战略地位。随着立法提案在失败中得到不断修正和完善，美国的网络安全法律体系也日渐清晰。这为我国的网络安全立法提供了有益借鉴。其一，注重顶层设计，制定我国网络空间安全中长期战略规划，为网络安全立法提供明确导向；其二，做好立法的全面规划，注重基础性立法的研究，保证立法与国家利益的一致性，同时要避免重复立法和分散立法，增强立法的协调性；其三，坚持国家网络空间安全与公民个人信息的同等保护原则，实现个人信息权益正当保护与国家网络空间安全有效守卫的平衡；其四，加强网络空间安全立法的国际合作，本着相互尊重和相互信任的原则，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系。

美国CERT组织架构、定位和作用浅析

1988 年，美国国防部高级研究计划署资助卡内基·梅隆大学（CMU）建立了第一个计算机应急响应组及协调中心（CERT/CC）。随后，美国国土安全部（DHS）又分别建立了美国国家计算机应急响应小组（US-CERT）和工业控制系统网络应急响应小组（ICS-CERT），美国军方以及其他民营部门也纷纷建立了 CERT 组织，满足自身对网络安全的需求。这里以 US-CERT 和 ICS-CERT 为主要对象，浅析美国 CERT 组织的架构、定位和发挥的主要作用。

一、美国 CERT 组织介绍及其架构

（一）US-CERT

美国国家计算机应急响应小组（United States Computer Emergency Readiness Team，US-CERT）于 2003 年成立，隶属于美国国土安全部。US-CERT 的宗旨是通过快速响应重大突发事件、分析威胁、与全球可靠的合作伙伴共享关键网络安全信息，为全美提供一个更安全和强大的互联网环境。US-CERT 致力于提升美国网络安全态势感知能力，协调网络信息共享，自发管理网络风险以保护美国公民权益。

US-CERT 保证“7×24 小时”不间断工作，接受、分诊并协调计算机紧急事件，为信息系统人员提供技术援助，并及时公布当前或潜在的安全威胁与漏洞信息。US-CERT 官网提供在线入口，可供漏洞发现者对紧急事件或软件漏洞以专用格式及时向 US-CERT 进行报告。此外，US-CERT 与关键基础设施所有者和运营商、学者、联邦机构、信息共享和分析中心（ISAC）、地方与各州的合作伙伴以及国内外相关机构共同提升网络安全态势感知能力。

US-CERT 将业务对象分为三大类：控制系统用户、政府用户、家庭和企业用户。面向控制系统的服务是为联邦、各州、地方中所有基础设施与关键资源部门解决工业控制系统安全问题，即控制系统安全项目（Control System Security Program，CSSP）。面向政府的服务主要是为各级政府部门提供关于网络安全的信息共享、安全协作与响应服务，其中比较重要的有“爱因斯坦计划”、“US-CERT 移动计划”，“国家漏洞信息数据库（NVD）”等。此外，US-CERT 也为个人或家庭、小型商业网络提供网络预警服务。

（二）ICS-CERT

工业控制系统网络应急响应小组（ICS-CERT）于 2009 年基于 US-CERT 的 CSSP 项目而成立，同样隶属于美国国土安全部。US-CERT 致力于与执法机构、情报组织以及联邦、地方等各级政府、控制系统所有商、运营商等合作减少关键基础设施的风险。此外，ICS-CERT 与各国和民营部门的 CERT 组织合作以分享有关工业控制系统的安全事件和补救措施的相关信息。ICS-CERT 六大工作任务包括：对于控制系统相关的突发事件进行回应和分析；对漏洞、恶意软件和数字媒体进行分析；提供现场的应急响应服务；以可操作情报方式提供网络态势感知；协调漏洞对外发布以及采取相应的补救措施；通过信息产品和警告方式分享漏洞和威胁信息。

ICS-CERT 的业务特征主要包括以下几项。

- **提供突发事件响应服务。**收到一个突发事件的报告后，ICS-CERT 将进行初步诊断以判断危害的程度。根据顾客的要求，ICS-CERT 可安排一个现场支持小组检查受影响机构的网络拓扑结构，识别受感染的系统，进行图像分析以及收集后续研究中所需的数据。ICS-CERT 可提供补救措施，为资产所有者和运营商提出建议以改善整体网络和控制系统的安全性。
- **设立高级分析实验室**（Advanced Analytic Lab，AAL）。ICS-CERT 设立高级分析实验室对受感染系统样本进行数字媒体和恶意软件分析。该实验室还有供应商设备的典型样本，可以在控制系统环境下对恶意软件进行功能测试和分析，并评估恶意软件的影响和关键基础设施漏洞导致的后果。
- **广泛合作促进信息共享和关键基础设施保护。**ICS-CERT 不仅同 US-CERT、国际组织和民营部门均有广泛的合作，还基于 CSSP 项目成立了工业控制联合工作小组（Industrial Control Systems Joint Working Group，ICSJWG），并同联邦控制系统安全工作组（Federal Control Systems Security Working Group）合作，共同促进信息共享和对关键基础设施与资源的保护。

（三）US-CERT 和 ICS-CERT 的架构

1. US-CERT 和 ICS-CERT 外部机构设置

US-CERT 与 ICS-CERT 均隶属于美国国土安全部（DHS），是美国国家网络安全和通信整合中心（NCCIC）的分支机构。

NCCIC 于 2009 年 11 月成立，由国土安全部网络安全与通信办公室（CS&C）主管，负责整合国土安全部下属的多个国家网络安全中心和应急响应小组，成为协调指挥美国网络安全各项行动的“中枢”。同时作为实施《国家网络应急响应计划》的主要负责部门，该中心是一个全天候的综合性网络安全和通信行动中心，是发生重大网络安全事件时协调相关行动的国家联络点和执行中心。同时 NCCIC 还作为信息的集成和分享中心，汇集和分享来自各合作伙伴的有关网络态势感知、脆弱性、入侵事件以及如何减少危害的信息。

DHS 架构图如图 1.2 所示，NCCIC 共下设 NCCIC 运营和整合中心（NO&I）、US-CERT、ICS-CERT 和国家通信协调中心（NCC）四个机构。

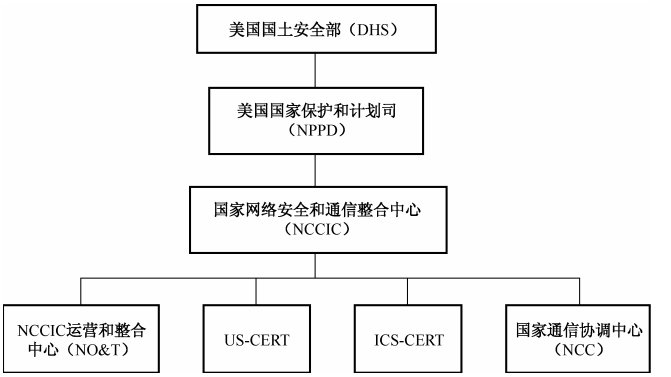

图 1.2　DHS 架构

2. US-CERT 内部机构设置

US-CERT 设立主任一名，负责全局的监管与组织工作（见图 1.3）。下设四个功能组，具体如下。

运营组：完成紧急事件的管理、检测与分析等业务。

协调整合组：负责协调与交流工作。

未来行动组：负责行动规划、技术方案的前瞻性研究。

资源管理组：完成员工及财务管理工作。

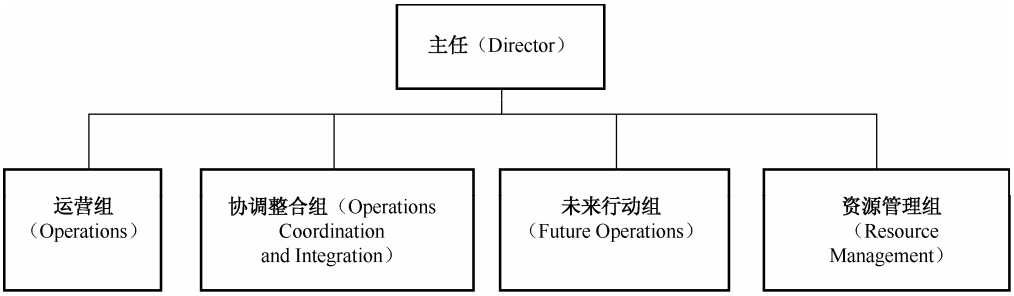

图 1.3　US-CERT 内部机构设置

二、美国 CERT 组织定位及其发挥的作用

（一）信息汇集中心——保持网络态势感知

2010 年 9 月，DHS 代表联邦政府制定并发布了《国家网络应急响应计划》（以下简称《计划》），该计划是非战争状态下由 DHS 主导的对国家级网络安全事件的应急响应。《计划》中以“联邦网络突发事件通道”表格的形式，明确了各个政府部门的职责和权限。其中 DHS 作为网络突发事件协调管理的中枢，负责在整个突发事件和所有合作伙伴中协调突发事件的管理活动。NCCIC 作为协调中心，是联邦政府、州和地方以及民营部门有关态势感知、漏洞、网络入侵、突发事件和补救措施的信息集中点。同时，NCCIC 作为外部利益相关方的支持者将在所有合作伙伴中提供多方向的信息共享。《计划》中明确提出，“为保持网络突发事件响应的及时和畅通，根据联邦规定，所有参与突发处理的部门和机构的信息必须通过 US-CERT 传送至 NCCIC，以便保持网络态势感知。”所有参与的组织机构应同 NCCIC 共同协调及响应。

在 DHS 2011 年 11 月发布的网络安全战略——《未来网络蓝图：美国国土安全部网络安全战略》中，提出了两大关键行动：保护关键基础设施信息和建立更为强健的网络生态系统。同时，为实现保护关键基础设施信息提出了四大目标：减少网络风险暴露的可能性、确保优先响应和修复、持续分享网络态势感知、增加系统弹性。在“持续分享网络态势感知”目标中，提出应充分发挥 US-CERT 发布网络安全警报和公告的职能，与美国国防部（DOD）、美国联邦调查局（FBI）、美国国家标准与技术研究所（NIST）等机构建立多元化合作，及时分享精确、可操作性强的网络警报信息。

US-CERT 还建立了国家网络感知系统（National Cyber Awareness System，NCAS），这是全球首个结合了识别、分析突发漏洞与威胁的全国性网络安全系统，为公众提供免费、实

时、可操作的计算机安全更新与警告信息。形式有警告、建议、公告。US-CERT 还运行着一个漏洞信息数据库，为 NCAS 发布的漏洞提供技术性描述。

（二）推动网络安全能力建设，提升公众意识

2011 年 5 月，奥巴马政府签署了《美国网络空间国际战略》（以下简称《战略》），该战略从建立网络安全政策、描绘网络空间未来、阐述重点政策和展望未来四个角度规划了美国网络空间发展。《战略》第二部分——“描绘网络空间未来”中提出了“构建繁荣和安全网络空间”的发展主题，表示美国将通过建立国外、双边和多边机构组织提升网络安全能力，从而使各个国家可保护本国的关键基础设施、加强全球性网络建设并为达成开放、彼此协作、安全可靠的网络共识而构建更亲密的伙伴关系。其具体实施措施包括建设技术性能力和网络安全能力两部分。

为提升网络安全能力，《战略》中指出：须借用 CERT 组织等机构在内的各个部门力量，用于扩大和调整专注于网络安全能力建设的计划，提升公众意识，开展法律和技术培训以及获得政策发展的支持。

（三）协同制定有效计划，打造全新网络部队

《美国国防部网络安全战略 2015》中，国防部提出构建一个全新的网络任务部队（Cyber Mission Force，CMF），提出将整合 CMF 成为一个更大的多任务美国军方力量，以达到跨域协同作用，确保 CMF 响应能力，并重构其军方和民用力量及基础设施，以便更好地执行 DOD 的任务。为此，强大的跨部门合作显得尤为重要。DHS 和军方 CERT 组织应与国防部设备提供商建立伙伴关系，为关键任务系统及相关支撑性的民用系统制定相应的具有连续性的防御计划。

（四）构建面向全球的监控网络

US-CERT 自 2003 年开始实施“爱因斯坦Ⅰ计划”，该系统能够自动收集、分析和共享美国政府部门之间的计算机安全信息，从而使各联邦机构能够实时感知其网络基础设施面临的威胁，以便更迅速地采取恰当的措施。“爱因斯坦Ⅱ计划”于 2007 年实施，该系统在原来对异常行为分析的基础上，增加了对恶意行为的分析能力，以使 US-CERT 获得更好的网络态势感知能力。自 2008 年开始，美国政府启动了国家网络安全综合计划（CNCI），其中的一部分就是“爱因斯坦Ⅲ计划”。至 2010 年，“爱因斯坦”系统已被部署到 19 个美国主要政府机构中的 15 个，其中包括美国国土安全部、司法部、交通部、国务院、财政部和教育部、美国联邦贸易委员会、美国证券交易委员会等部门。“爱因斯坦Ⅲ”系统不仅被部署在整个联邦政府网络中，而且被部署到公共互连网络中，其主要创新在于强调面向网络的实时态势分析、威胁感知、主动防御。美国政府期望通过“爱因斯坦”计划的实施，首先能够保护美国国内重要的网络信息资产，同时还能感知监控他国互联网应用，使其成为主动防御甚至反制工具，最终成为美国国家安全战略体系中的重要组成部分。

（五）保护关键基础设施

ICS-CERT 是美国针对工业系统关键基础设施的网络攻击所成立的专门性应急响应机

构，为控制系统环境应对各种网络威胁提供具有可操作性和有针对性的防御。ICS-CERT 对与工业系统相关的突发事件、漏洞、恶意软件等进行回应和分析，也提供面向基础设施的安全服务。

（六）成为网络安全交流平台

US-CERT 是普通公民、企业和其他国际、国内组织机构直接与美国政府就网络安全进行交流和协调的重要平台，具有推进政府与企业参与国家信息安全应急管理的职能，在国家信息安全协同治理中发挥重要作用。

第二章　美国网络安全战略概要

《关键基础设施和重要资产实体保护国家战略》摘要

《关键基础设施和重要资产实体保护国家战略》（以下简称《战略》）是《国土安全战略》与国土安全部拟制定的“国家保护计划”之间的重要桥梁。《战略》明确指出了美国在保护关键基础设施及重要资产方面所要实现的战略目标，并提出了为实现这些目标有关各方所应遵循的基本指导原则。此外，它还明确了美国近期的保护重点及相关措施，并公开了“资源分配程序”。最重要的是，《战略》为建立一个全国性的、由各级政府（联邦、州、地方）和民营企业共同参与的协作机制奠定了坚实的基础。

一、战略目标

（1）对关键基础设施及重要资产进行界定，即从是否会影响到整个国家的公共卫生、安全及管理，以及是否会影响到国民经济、国家安全和公众信心的角度出发，确定哪些基础设施和资产属关键基础设施和重要资产。

（2）当关键基础设施和重要资产面临威胁时，及时发布警报并予以有效保护。

（3）采取具体措施，建立一个全国性的、由各级政府（联邦、州、地方）和民营企业共同参与的协作体系，以确保其他可能成为犯罪分子未来攻击目标的基础设施和资产得到有效的保护。通过协作，各级政府和民营企业能够更好地保护各自所管辖或拥有的基础设施和资产。

二、国土安全和基础设施保护：共同的责任

为保护关键基础设施和重要资产，需要建立一种全新的国家协作模式。“国土安全”的基本原则完全不同于传统意义上的国家安全原则。过去，人们一向认为，国家安全是联邦政府的职责。但“国土安全”却是各方共同的责任，仅靠联邦政府是无法完成这一使命的，特别是在关键基础设施和重要资产保护方面。各级政府（联邦、州及地方）、民营企业和有关的个人必须步调一致、共同努力，才能完成保护“国土安全”的重要使命。

为防止关键基础设施和重要资产被恐怖分子利用，必须掌握恐怖分子的动机、攻击目标及其惯用的战术。与此同时，还必须对受保护的基础设施和资产中存在的弱点以及排除或缓解这些弱点所面临的各种挑战进行全面的评估。这是一项需要整个国家协同配合、共同努力

才能完成的任务。

（一）关键基础设施的构成及其重要性

关键基础设施关系到国家的安全、管理、经济运转、人民生活方式乃至美国的形象和民族自豪感。这些关键基础设施是由众多高级且复杂的设施、系统和功能组成的，既包含了人力资产（human assets），也包含了物理及计算机网络系统，还包含了一些基础设施的正常运转所必不可少的重要节点。关键基础设施行业包括：农业和食品、水利、公共卫生、紧急救援服务、国防工业、电信、能源、交通、银行和金融、化工及危险材料、邮政和船运。

（二）重要资产的构成及其重要性

重要资产和重大场合也是恐怖分子的主要攻击对象。一旦遭到攻击，不仅会造成大量的人员伤亡和财产损失，而且会严重损害国家的威望、公众的士气和信心。除核电站和大坝之外，重要资产还包括那些象征美国传统价值观、制度或美国政治、经济实力的标志性建筑或设施，如政府设施、国家纪念碑和历史名胜等。当有大型公众庆祝活动或其他重大事件发生的时候，这些资产更容易成为恐怖分子的攻击目标。

三、国家政策和指导原则

《战略》重申了美国长期坚持的保护关键基础设施及重要资产的国策，并提出了 8 项旨在支撑国内保护战略的指导原则。

（1）保护公共安全，维护公众信心，保证公共服务。

（2）建立责任机制。

（3）鼓励并推动各级政府之间、政府与业界之间的合作。

（4）鼓励市场解决方案，一旦市场解决方案未能奏效，政府将积极干预进行补救。

（5）促进信息共享。

（6）加强国际合作。

（7）改进反恐技术，提高相关技能。

（8）维护公民隐私权及其他宪法所赋予的权利。

四、组织框架及协作体系

实施《关键基础设施和重要资产实体保护国家战略》，不仅需要一个统一的组织框架、一个明确的目标和一套清晰的协作程序，而且组织内的每一位成员必须了解自己所扮演的角色、所承担的责任和义务。建立稳固、统一的组织体系有利于各级政府之间、各级政府和民营企业之间进行有效的合作。否则，它们将无法完成国内保护政策的协调与统一、统筹规划、资源配置、绩效评估及其他各项任务。

（一）联邦政府的责任

在国土安全方面，联邦政府有以下主要职责。

（1）对关键设施、系统及其运行情况进行评估与监测。

（2）确保各级政府及民营企业协同保护国家关键基础设施和重要资产。

（3）提供并整理各种与恐怖活动有关的信息和评估，及时向州、地方政府及民营企业合作者发布恐怖威胁警报。

（4）制定并实施全面、多层次的保护政策和计划。

（5）制定跨行业、跨行政区域的保护标准、指南和协议。

（6）大力推广在关键基础设施和重要资产保护方面的好的做法、程序以及弱点评估方法。

（7）开展示范项目。

（8）开展全民教育，提高人们对关键基础设施和重要资产的保护意识。

（9）提高联邦政府与州、地方政府的快速反应队伍（responders）以及服务提供商协同作战的能力。

根据《国土安全国家战略》所确立的组织框架，国土安全部作为主管关键基础设施和重要资产保护工作的联邦机构，对各级政府和民营企业在此方面的工作进行跨行业的总体协调。此外，它还负责进一步完善并实施本《战略》中的核心内容。

（二）州、地方政府的责任

在关键基础设施和重要资产保护方面，美国所有的州及地方政府都将承担各自的责任。与联邦政府一样，它们必须对其拥有并运营的关键基础设施和重要资产进行界定，并予以有效保护。州政府还应当在指定的联邦主管部门和机构的通力协作下，推动下级地方政府在应急反应和资源支持等方面开展合作。

（三）民营企业的责任

民营企业拥有并经营着大多数关键基础设施和重要资产。在当前情况下，它们仍旧是保护自身设施的第一道防线。因此，民营企业应当重新评估并调整自己的商业计划、保险和投资项目，以更好地应对不断升级的恐怖威胁。

《国家网络安全战略》概要

一、概述

美国国家关键基础设施由公私机构组成，分布在以下部门：农业、食品、供水、公共卫生、应急服务、政府、国防工业基地、信息与通信、能源、交通、银行与金融、化学与危险品、邮政与运输等。网络是这些部门的神经系统，即整个国家的控制系统。成千上万互连的计算机、服务器、路由器、交换机以及光缆一起构成了整个网络空间，并使我们的关键基础设施得以运行。因此，网络的正常运作对经济及国家安全至关重要。

《国家网络安全战略》是保护国家安全工作的一部分。它是《国家国土安全战略》的组成部分，并由《关键基础设施和重要资产实体保护国家战略》所补充。《国家网络安全战略》的目的是使美国人能够保护自身拥有、操作、控制或者对其有影响的网络。网络安全是一项艰巨的战略挑战，它要求整个社会，包括联邦政府、州与地方政府、民营行业以及美国人民的共同协作与努力。

《国家网络安全战略》概括出了网络安全在组织与程序上的初始构架。它为联邦政府部门及机构在网络安全中发挥作用指明了方向，同时，还确定了州及地方政府、民营企业与组织、美国公民个人对整个网络安全进行改进的步骤。战略计划强调了公民营机构共同参与的作用，为所有人保护自身的网络安全提供了框架。网络的动态性要求安全战略计划要随着时间的推移进行调整与补充。

网络攻击的快速与匿名性使其区别于恐怖行为及犯罪行为，因此要借助《国家网络安全战略》减少国家的网络安全漏洞，并削弱针对关键信息基础设施或者支持这些设施的重要资产所发起的攻击。

二、战略目标

与《国家国土安全战略》相一致，《国家网络安全战略》的战略目标是：

（1）阻止针对美国关键基础设施实施的网络攻击；

（2）减少国家网络安全漏洞；

（3）使受到网络攻击后的损失最小、恢复时间最短。

三、网络安全优先发展五大重点

《国家网络安全战略》包括五大部分：一是国家网络安全响应系统，二是国家网络安全威胁和漏洞缩减计划，三是国家网络安全意识和培训计划，四是各级政府的网络安全保障，五是国家安全和国际网络安全合作。第一部分着重于提高我们对网络事故的响应能力，减少此类事故可能带来的破坏。第二、第三和第四部分旨在减少网络攻击带来的威胁以及自身漏洞。第五部分旨在防止可能破坏国家安全资产的网络攻击，以及提高国际社会对此类攻击的

管理和响应能力。

（一）国家网络安全响应系统

《国家网络安全战略》确定了进行网络安全响应的八项主要行动和计划。

（1）建立一个公私合作框架，对国家级的网络事故做出响应。

（2）提供网络攻击的战术战略分析和漏洞评估的发展情况。

（3）鼓励民营行业发展对网络状况的分析能力。

（4）拓展“网络预警和信息网”，支持国土安全部在协调网络危机管理中发挥作用。

（5）加强国家事故管理。

（6）协调各界自愿加入全国性的、国有和民营部门共同参与的各类连续性计划和应急计划。

（7）为联邦系统试验网络安全连续性计划。

（8）改进和加强公立及民营部门双方在网络攻击、威胁和漏洞等方面的信息共享。

（二）国家网络安全威胁和漏洞缩减计划

《国家网络安全战略》确定了减少网络安全威胁和相关漏洞的八项主要行动和计划。

（1）增强执法部门在防止和起诉网络攻击方面的能力。

（2）建立一套国家漏洞评估程序，以更好地理解威胁和漏洞的潜在后果。

（3）通过改进协议和路由保证互联网架构的安全。

（4）推动对信任数字控制系统/监督控制和数据获得系统的使用。

（5）减少和修补软件漏洞。

（6）了解基础设施的相互依靠性，改进网络系统和电信设施的物理安全性。

（7）优先考虑联邦网络安全研发议程。

（8）对新系统进行评估并保证其安全性。

（三）国家网络安全意识和培训计划

《国家网络安全战略》确定了推动网络安全意识、教育和培训的四项主要行动和计划。

（1）推动建立一个综合性的国家预警项目，使所有的美国人（包括企业、劳动者和公众）能够确保其个人网络空间的安全。

（2）扶持适当的培训和教育计划，以满足国家的网络安全需要。

（3）提高现有的联邦网络安全培训计划的功效。

（4）推动民营部门对具有良好协调性、得到广泛认可的专业网络安全认证的支持。

（四）各级政府的网络安全保障

《国家网络安全战略》确定了保证各级政府网络安全的五项主要行动和计划。

（1）对联邦网络系统面临的威胁和存在的漏洞进行持续的评估。

（2）对联邦网络系统的授权使用者进行认证和维护。

（3）保证联邦无线区域性网络的安全性。

（4）增强政府外包和采购的安全性。

（5）鼓励各州和地方政府考虑建立信息技术安全项目，并参与同级政府之间的信息共享，共同建立分析中心。

（五）国家安全和国际网络安全合作

《国家网络安全战略》确定了加强美国国家安全和国际合作的六项主要行动和计划。

（1）加强与网络有关的情报工作。

（2）提高对网络攻击进行定性并做出反应的能力。

（3）加强美国国家安全团体的内部协作，共同对网络攻击进行回应。

（4）与业界合作，并通过国际组织推动国际上公立部门及民营部门之间的对话和合作，保护信息基础设施，推动全球性的“安全文化”。

（5）推动建立国家性和国际性的监视及预警网络，发现并防止网络攻击。

（6）鼓励其他国家加入《欧洲议会网络犯罪公约》，并确保这些国家的法律及程序具备《公约》的广泛性。

四、国家努力

保护分布广泛的网络资产需要美国民众的努力。仅靠联邦政府不足以保护美国的网络安全。我们的联邦主义和有限政府的传统要求联邦政府之外的组织发挥主导作用。政府鼓励每一位有能力的美国公民对网络安全作出贡献。联邦政府欢迎建立或参与公私合作关系，提高网络安全意识，培训员工，刺激市场力量，改进技术，确认并补救漏洞，互换信息，以及制定复苏计划。

美国人民和组织已经采取了一些步骤加强网络安全。2002 年 9 月 18 日，众多民营私人机构公布了保证各自基础设施安全的计划和战略。“关键基础设施安全合作委员会”在促进民营行业服务于《国家网络安全战略》方面发挥了独特作用。各关键部门的网络安全战略计划可参见 http://www.pcis.org。这些综合性基础设施计划描述了各部门的战略计划，包括：银行和金融业、保险业、化学、石油和天然气、电力、执法部门、高等教育、运输（铁路）、信息技术和通信、水务。

随着各关键基础设施部门实施这些计划，我们的设施面临的威胁和存在的漏洞必将减少。

五、结论

我们对网络空间的依赖程度将不断提高。互联网支持经济发展，为国土防卫提供保障。我们将长期不懈努力保护网络安全。

保护网络安全是一项复杂且不断发展的任务。《国家网络安全战略》是在主要经济部门、州、地方政府、大学以及相关组织的共同协作下制定的。起草过程中，公众评论也受到了重视。

建立公私合作关系响应了总统的号召，双方制定了保护其网络安全的战略。这个独特的合作和过程是必要的，因为国家大部分的网络资源都由政府以外的机构控制。随着网络安全战略的实施，更多的部门投资控管被纳入计划。因此，有关加强网络安全的对话将继续下去。

《国家网络安全战略》是保护信息基础设施的长期努力的第一步。联邦执行机构将通过

各种手段实现该战略。行政部门将协同国会在该战略的基础上起草进一步的联邦安全预算。各领导部门和机构将有计划地实施战略分配的任务。

国土安全部将在战略实施中扮演重要角色。除了执行战略分配的任务，国土安全部将作为州和地方政府、私人部门以及与网络安全有关的美国人民的联邦连接点，还将同白宫合作，协调并支持战略中推荐的非联邦任务。

各部门都将负责各自的网络安全事宜。联邦政府将以实际举措，以及对州和地方政府的鼓励措施，评估战略中列出的网络安全项目的有效性。措施允许各机构调节其进度，决定资源分配，从而调整优先策略。

联邦、州、地方政府、组织以及美国人民将继续为提高网络安全能力而努力。随着这些战略和计划的执行，将极大地减少威胁和攻击。

网络安全和个人隐私不相冲突。网络安全计划必须加强，而不是减弱。联邦政府将继续定期会同隐私保护者探讨网络安全及该战略的实施。

在可预知的未来，两件事情将得到落实：依靠网络，联邦政府将寻求与民营行业持续广泛地合作；发展、贯彻、完善《国家网络安全战略》。

美国解密《国家网络安全综合计划》中的 12 项提议

2010 年 3 月 2 日，奥巴马政府对前任总统布什政府制定的一份美国网络防御战略，即《国家网络安全综合计划》（CNCI）的部分内容进行了解密。白宫互联网安全协调官霍华德·斯密特对该计划的一些内容进行了描述，他表示，这一解密是兑现奥巴马总统有关执政透明的承诺。

CNCI 包括了许多互助性的提议以实现下面 3 个重要目标，进而保护美国的网络空间安全。

（1）通过在联邦政府（最终落实在州、地方和部族政府以及民营领域合作者）内部创建并加强对网络漏洞、威胁和事件的共享态势感知能力，以及减少当前漏洞和防止入侵的快速反应能力，进而建立起抵御当前面临的迫切威胁的防线。

（2）加强美国的反情报能力并增进关键信息技术供应链的安全，进而实现应对全方位威胁的防御能力。

（3）通过扩大网络教育、协调和重新定位整个联邦政府内的研发工作、致力于明确和制定相关战略以阻止敌对和恶意的网络空间行为等措施，进而巩固未来的网络空间环境安全。

该计划共列出了 12 项提议，具体内容如下。

（1）将现有的美国联邦政府各部门的网络合并成唯一的、接入“可信互联网连接”的政府网络。由美国国土安全部、美国行政管理和预算局牵头的“可信互联网连接计划”（TIC）将合并美国联邦政府部门网站的外部接入点，包括美国联邦政府网络与外部互联网的连接。这一合并将为美国联邦政府的网络提供一个共同的安全解决方案，包括：推动减少外部接入口、建立安全基线的能力、为遵守安全能力的相关机构提供验证等。

（2）在联邦政府组织中部署一个传感器入侵监测系统，又称“爱因斯坦Ⅱ计划”。当未经授权的用户试图进入联邦政府部门的网络时，入侵监测系统将会发出预警，这将成为保护美国政府网络的重要组成部分。为此，美国国土安全部正在部署建设基于签名的传感器入侵监测系统，这种传感器通过对进入联邦政府的网络流量进行监测，能够发现未经授权进入美国联邦政府网络的潜在恶意活动。在对技术进行投资的同时，该计划还提出加大对网络人员专业基础培训的投入，以满足完成国土安全部网络安全扩展任务的需要。“爱因斯坦Ⅱ计划”能够向美国计算机应急响应组织（US-CERT）实时报告联邦政府网络流量中的恶意行为或可能的恶意行动，并可提供源数据的相关性和可辨性，这将极大地提高 US-CERT 分析师对网络环境的认知能力，增强其处置联邦政府网络安全的弱点和漏洞的能力，并使 US-CERT 能够更加有效地与美国各级政府的网络安全防御部门、民营部门的安全专家以及美国公众分享相关的安全信息。

（3）在联邦政府组织中部署入侵防范系统，又称“爱因斯坦Ⅲ计划”。这一提议旨在保护美国民用部门和联邦行政部门机构的网络安全。它将吸收商业技术和专门的政府技术，对进出联邦行政机构网络的所有数据包进行实时检查，并判断其是否具有威胁性。“爱因斯坦Ⅲ计划”的目标是确认恶意网络流量并鉴别其特性，以加强网络安全分析能力、安全态势感

知及安全响应能力。“爱因斯坦III计划”将协助国土安全部和 US-CERT 防卫、保护并减少联邦行政部门网络和系统的脆弱性。美国政府将对这一计划进行大量和长期的投资，以加强发现外国网络攻击的国家情报能力。国土安全部目前正在对“爱因斯坦III计划”进行测试工作，以检验其是否具备该计划所描述的基于美国国家安全局开发的技术的能力。政府公民自由和隐私官员也正与国土安全部及 US-CERT 密切合作，以在“爱因斯坦III计划”制定和应用部署中建立适当的和必要的隐私保护措施。

（4）协调并指导相关的研究开发活动。个人或组织并未意识到所有与网络相关的研发工作都是政府的资助。该提议制定策略和建立架构以协调所有美国政府资助或进行的网络研发工作，包括涉密的和非涉密的，并对所需的研发工作进行重新定向。这将有助于消除联邦政府对网络安全研究的重复投资，并有助于确定研究差距、突出研发重点，确保在制订战略投资计划时使美国纳税人的钱能够落到实处。

（5）连接现有的网络运行中心以加强对网络安全态势的认知能力。由于目前针对联邦系统的恶意行动日益增多，因而保证政府信息安全办公室与战略运行中心能够实现信息共享尤为迫切，只有这样才能更好地了解针对政府系统的整体威胁状况，并在保护个人隐私及其他受保护信息法律法规允许的情况下，最大限度地利用各部门特有的能力以形成最佳的网络防御。该提议将为负责开展美国网络活动的 6 个中心提供必要的手段，使它们彼此之间能够实现对网络安全态势认知的共享及协作。在这个提议中，隶属于美国国土安全部的国家网络安全中心（NCSC）将在确保美国政府网络和系统安全中发挥主导作用。NCSC 将根据这一提议，对上述 6 个中心进行协调和整合以提供跨领域安全情况通报，并对美国国家网络和系统进行分析和报告，促进机构内部的合作和协调。

（6）制定并推行政府部门间的网络反间谍（CI）计划，以便协调联邦各政府部门进行监测，阻止和减少外国网络间谍机构对美国政府和私人领域进行网络情报威胁。为达到上述目标，该计划将建立和扩展网络反间谍教育和认知项目，并增加工作人员，从而将 CI 整合进所有的网络运作和分析中，增强雇员对网络反间谍威胁的意识，并增强各级政府部门的反间谍协作。

（7）加强涉密网络的安全性。涉密网络存储了联邦政府最敏感的信息，并能够确保至关重要的战争、外交、反恐、立法、情报及国土安全行动的实施。对这些网络的入侵和破坏将给国家安全带来难以估量的严重后果。因此必须对涉密网络及其存储的数据审慎地评估，以确保涉密网络及其数据的安全性。

（8）加强网络教育及培训。尽管美国政府在新科技上投入数以亿计的资金以确保美国政府在网络空间的安全，但只有拥有正确的知识、技巧及能力的人来运用这些科技才是成功的关键。美国联邦政府、民营行业都缺乏足够的网络安全专家来落实《国家网络安全综合计划》，而且也未充分形成联邦网络安全职业制度。现有的网络安全培训和人员发展计划在总体上是良好的，但关注范围过于局限且缺乏行动的一致性。为了继续保持美国的科技优势和未来的网络安全，美国必须培养精通科技和网络的人才，并为未来的员工提供有效的人才输送渠道。这就需要制定类似于 20 世纪 50 年代升级科学和数学教育的国家战略，以迎接这一挑战。

（9）明确和制定持久的“跨越式进步”技术、战略和项目。CNCI 的目标之一就是开发新技术，从而在现有系统的基础上不断提升网络安全的量级并在未来 5～10 年内部署。这项提议能制定战略和计划以优化政府在研发方面对关键网络安全问题追求高风险/高回报解决

方案的职责。联邦政府已经开始为研究机构勾勒出挑战框架，寻求外部智囊的帮助来解决这些难题。美国政府正与民营机构进行交流，确认双方的共同需求，推动双方在重点研究领域进行投资。

（10）制定和发展持久的震慑战略和计划。美国的高级决策者必须考虑可供政府参考的多种长期战略选择，以确保网络空间不对美国的安全造成影响。当下，美国政府在网络安全问题上一直采取传统的方法，但这些方法并未达到所需的安全保障级别。该提议的目的在于通过改善预警能力、明晰民营企业和国际伙伴所扮演的角色、发展国有和非国有部门的响应能力等措施来建立网络防卫战略，以阻止对网络空间的干扰和攻击。

（11）制定多管齐下的全球供应链风险管理模式。商业信息和通信科技市场的全球化，给企图损害美国利益的国家、个人提供了更多的机会，他们可以在未授权的情况下通过渗透供应链获取和更改数据，或对通信进行干扰。要应对这类来自国内和全球化供应链中产生的风险，必须在产品、系统和服务的整个生命周期中采取一种战略性和综合性的方式。要应对这类风险，美国须提高对威胁、脆弱性，以及与采购决定相关后果的认知；开发和应用各种工具和资源，在技术上和运作中减少在产品整个生命周期（从设计到退出市场）中产生的风险；制定新的采购政策和运作方式以应对市场全球化的复杂性；与工业界合作发展并应用供应链风险管理标准和最佳操作方式。这一提议将改善联邦政府的技能、政策能力和处理流程，为各部门和机构提供更好的方法管理和减少供应链风险，从而减小联邦政府部门和机构所面临的系统网络风险。

（12）确定联邦政府在将网络安全融入关键基础设施工作中的职责。美国政府与控制关键基础设施的民营企业互有需求，不可分割。这项提议建立在联邦政府与关键基础设施和重要资源（CIKR）的公民营领域所有者和运营商之间已经建立并正在发展的伙伴关系之上。国土安全部与其民营行业合作方已制定了一个具有里程碑意义的积极的共享行动计划，包括短期和长期建议，特别是吸收和利用了以前取得的成果和经验，加强了关键基础设施和重要资源部门的安全弹性及运作能力。一旦政府部门、关键基础设施和重要资源遭受网络威胁或发生网络安全事故，政府部门和民营行业将共享信息。

《国家基础设施保护计划》概要

确保国家重要基础设施和关键资源（CIKR）的应急恢复是国家安全、公众健康、经济繁荣和生活稳定的核心。对重要基础设施和关键资源的攻击可能严重破坏政府和产业的运行，所引起的连锁反应将广泛波及事件中的目标区域及物理位置之外的更大领域。直接的恐怖袭击和自然、人为或者源自技术的威胁将会在造成人员伤亡、财产破坏和经济影响等灾难性损失的同时，深深挫伤公众的士气和信心。利用国家重要基础设施和关键资源的构成要素作为大规模杀伤性武器发动袭击，甚至会给国家的财产和人们的心理造成毁灭性的灾难。

一、引言

《国家基础设施保护计划》（NIPP）的总体目标是预防、阻止、抵消或者减轻恐怖分子的故意破坏行为或者恶意利用国家重要基础设施和关键资源的行为。要加强国家在恐怖袭击、自然灾害和其他紧急事件中充分准备和及时响应，以及快速恢复重要基础设施和关键资源的能力，建设更为安全、安定和更具恢复能力的美国。

《国家基础设施保护计划》提供了统一的机制，将现有和未来的重要基础设施和关键资源保护和恢复战略整合为统一的国家计划，并付诸行动。《国家基础设施保护计划》框架支持在各部门之间实现优先保护、恢复预案和投资，确保减少薄弱环节、阻止威胁并将恐怖袭击和其他人为以及自然灾害的后果降低到最小限度，从而实现缓解风险带来最大获益的同时，政府和民营部门的资源可用。《国家基础设施保护计划》风险管理框架识别并建立了现有的公共和私人部门保护计划以及恢复能力战略，发挥投资效益，将重要基础设施和关键资源所有者和运营者的风险降低到最小限度。措施包括：降低重要基础设施和关键资源资产、系统、网络、功能或者其他网络互联带来的总体风险，制止威胁、缓解薄弱环节或者将恐怖袭击及其他突发事件所造成的严重后果降低到最小限度（见图 2.1）。保护措施还包括一系列的工作，例如完善安全协议、强化设施、建立恢复力和冗余性、将隐患抵御能力整合到设施设计中去、主动或者被动的策略、安装安全系统、利用“自我复原”式技术、推广劳动力保障计划、网络安全措施、培训和演练、业务连续性计划、复原和恢复措施等。

为了实现《国家基础设施保护计划》的总体目标，要采取相应措施来实施一系列的具体目标，包括：

（1）理解和恐怖袭击以及其他隐患有关的信息，与重要基础设施和关键资源合作伙伴共享这些信息；

（2）建立合作伙伴关系，共享信息，实施重要基础设施和关键资源保护计划；

（3）实施长期风险管理计划；

（4）充分利用相关资源，保护、恢复和复原重要基础设施和关键资源。

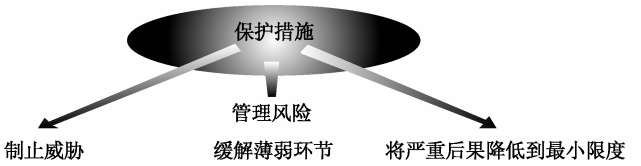

图 2.1　保护措施

这些具体目标要求重要基础设施和关键资源合作伙伴之间建立协调性合作伙伴关系，其中包括：联邦政府，各州、地方、部族和区域政府，区域同盟，民营部门，国际机构，非政府组织。《国家基础设施保护计划》提供了基本框架，其中定义了一系列灵活的程序和机制，这些重要基础设施和关键资源合作伙伴可以使用这些程序和机制实施国家计划，实现对各个部门重要基础设施和关键资源的长期保护。

二、职权、使命和责任

2002 年通过的美国国土安全法案（Homeland Security Act），为美国国土安全部（DHS）负责保护国家的重要基础设施和关键资源提供了法律依据。法案指定美国国土安全部制订保护重要基础设施和关键资源的综合性国家计划，建议与联邦政府的其他机构协调行动，与州及地方政府机构或者部门、民营部门及其他团体合作。

第 7 号国土安全总统令（HSPD7）建立了统一框架，提供了国家保护重要基础设施和关键资源的途径。此命令确立了美国“强化国家重要基础设施和关键资源保护”的政策，并且批准启动了国家计划。在第 7 号国土安全总统令（HSPD7）中，总统任命国土安全部部长作为“领导联邦政府和机构、各州和地方政府以及民营部门对重要基础设施和关键资源进行保护的首席联邦官员”，并且指派联邦特定部门机构（SSA）负责保护重要基础设施和关键资源（见表2.1），并为建立或者补充相关部门提供了标准。根据第7号国土安全总统令（HSPD7），《国家基础设施保护计划》明确了合作各方在开展重要基础设施和关键资源保护活动方面的角色和责任，并要求尊重和整合这些合作伙伴的职权、管辖权和特权。

重要基础设施和关键资源合作伙伴的主要使命如下。

美国国土安全部：协调国家在重要基础设施和关键资源方面的总体工作，对《国家基础设施保护计划》的编制和实施进行监督，并整合国家的前瞻性措施。

特定部门机构：实施《国家基础设施保护计划》框架，并根据每个重要基础设施和关键资源部门的具体特征给予指导和调整。

其他联邦部门、机构和办公室：落实第 7 号国土安全总统令（HSPD7）以及其他相关法令、执行命令和政策指令所赋予的、对重要基础设施和关键资源的保护使命。

各州、地方、部族和区域政府：作为国土安全总计划的组成部分，根据《国家基础设施保护计划》风险管理框架编制，实施重要基础设施和关键资源保护计划。

地区合作伙伴：利用跨权限、跨部门的合作，在一定的地理区域内对重要基础设施和关键资源开展保护。

董事会、委员会、权力当局、政务会及其他实体机构：基于重要基础设施和关键资源的各个方面，跨部门和跨权限地发挥监管、咨询、政府或者业务监督职能。

民营部门所有者和运营商：针对重要基础设施和关键资源，开展保护、恢复、协调和合

作活动，并为各级政府提供意见、建议和专业知识。

国土安全咨询委员会：针对保护政策和活动，向政府提供意见、建议和专业知识。

学术界和研究中心：针对重要基础设施和关键资源保护工作，提供专业知识、独立分析、研发（R&D）和教育计划。

表 2.1　特定部门机构和指定的重要基础设施和关键资源部门

特定部门机构	重要基础设施和关键资源部门
农业部[a] 卫生和公共服务部[b]	农业和食品
国防部[c]	国防工业基础
能源部	能源[d]
卫生和公共服务部	医疗和公共健康
内政部	国家遗迹和象征
财政部	银行和金融
环保署	水务[e]
国土安全部 基础设施保护办公室	化学、商业设施、关键制造业、大坝 应急服务、核反应堆、物料和废物
网络安全和通信办公室	信息技术通信
交通运输安全管理局	邮政和航运
交通运输安全管理局 美国海岸警卫队[f]	交通运输系统[g]
移民和海关执法局 联邦保护服务	政府设施[h]

注：[a]农业部负责农业和食品（包括肉类、禽类和蛋类产品）；

[b]卫生和公共服务部负责除了肉类、禽类和蛋类产品之外的其他产品；

[c]本计划内的任何内容都不会削弱或者影响国防部部长的职权，包括作为统帅的总统到国防部部长再到军队指挥官对于军队的连锁指挥系统或者军事命令和控制程序；

[d]能源部包括生产、精炼、存储和分配石油、天然气和电力资源，商业性的核电设施除外；

[e]水务部包括饮用水和废水处理系统；

[f]美国海岸警卫队是负责海事运输的特定部门机构；

[g]正如第 7 号国土安全总统令（HSPD7）所述，交通部和国土安全部会就涉及交通运输安全和交通运输基础设施保护等方面的各项事宜开展合作；

[h]教育部是政府设施部门下教育设施分部所属的特定部门机构。

三、重要基础设施和关键资源保护项目战略：风险管理

《国家基础设施保护计划》的基础是其风险管理框架（见图 2.2），该框架建立了结合事件后果、薄弱环节和威胁信息等因素，生成国家或者地区风险的评估结果的全过程。

设计这一风险管理框架是为了集中采取一系列行动，持续推动和加强对重要基础设施和关键资源的保护。这些活动包括：设定总体和具体目标，确认重要资产、系统和网络，根据事件后果、薄弱环节和威胁信息评估风险，根据风险评估结果或者在减轻风险方面的投资回报分析结果确定工作重点，执行保护计划和恢复策略，评估项目取得的成效等。

实施以上过程将帮助降低重要基础设施和关键资源所面临的风险，提高管理的灵活性。根据个别重要基础设施和关键资源部门的根本特征，基于相应资产、系统、网络或任务，对《国家基础设施保护计划》进行调整。美国国土安全部（DHS）、特定部门机构（SSA）以及其他的重要基础设施和关键资源合作伙伴会在实施风险管理框架方面共担责任。

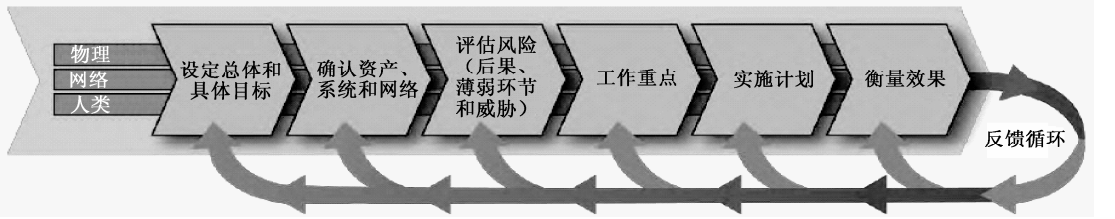

图 2.2　《国家基础设施保护计划》风险管理框架

四、重要基础设施和关键资源保护项目的组织和合作

由于国家重要基础设施和关键资源的庞大和复杂性，国内保护性建筑的分布特征，以及恐怖袭击、人为或者自然灾害的不确定性，如何采取有效的保护和恢复措施已经成为一项重要挑战。为了确保这类措施的有效性，《国家基础设施保护计划》要求建立能够确保信息共享与保护的组织结构和伙伴关系，实现既定目标。

《国家基础设施保护计划》定义了一种组织结构，这种结构可以为各级政府以及各部门内外在保护重要基础设施和关键资源所进行的协调努力方面，提供基本框架。通过为各部门建立的协调委员会，实现特定部门的计划和协调。部门协调委员会（SCC）由各个所有者和运营商代表组成，他们通常来自民营部门。政府协调委员会（GCC）由各个特定部门机构（SSA）代表，其他联邦政府和机构代表，各州、地方、部族和区域政府代表组成。这些委员会创建了一种机构，通过这个机构，来自各级政府和民营部门的代表可以协作或者共享现有的重要基础设施和关键资源保护途径，共同努力完善职能。参与并实现与外国政府以及国际组织机构之间的协调，这对于确保实现美国国内外重要基础设施和关键资源的保护和恢复也至关重要。《国家基础设施保护计划》提供了相应机制和程序，从而使得美国国土安全部、美国国务院、美国特定部门机构及其他的合作伙伴强化国际合作，支持重要基础设施和关键资源的保护工作和措施。

美国国土安全部会与所建立的跨部门实体机构开展合作，促进重要基础设施和关键资源部门在特定地理区域范围内实现协调、沟通和共享。相关性分析通常十分复杂，必须具备建模和模拟能力。部门协调委员会可以通过由部门协调委员会领导层组成的重要基础设施和关键资源跨部门委员会，来处理跨部门问题和相关问题。重要基础设施安全合作伙伴将通过美国国土安全部重要基础设施和关键资源执行秘书处，对此提供支持。政府协调委员会会通过由《国家基础设施保护计划》联邦高级领导委员会（FSLC），各州、地方、部族和区域政府协调委员会（SLTTGCC）组成的政府跨部门委员会，来处理跨部门问题和相关性问题。此外，区域财团协调委员会（RCCC）还将为基于区域利益而保护重要基础设施和关键资源的机构提供论坛。

基于互惠互利、相互信任关系的有效信息共享和信息保护程序，可以帮助确保重要基础设施和关键资源保护计划及行动的有效实施、统筹协调。信息共享可以同时帮助政府和民营部门合作伙伴对事件进行精确评估，设计风险评估，并确定适当的行动步骤。《国家基础设

施保护计划》使用信息共享网络的方式构建一种全新的模型：重要基础设施和关键资源合作伙伴共享和保护分析风险和做出风险知情决策所需的信息。网络途径能够实现政府和行业之间安全、多维度的信息共享。这种途径提供了一种机制，按照要求使用信息保护协议来支持战略和特定威胁评估、威胁警报、事件报告、隐患后果评估、风险评估和最佳实践的发展和共享。这种信息共享途径使得重要基础设施和关键资源合作伙伴可以评估风险、识别和优化风险管理机会、分配资源、开展风险管理活动，并且持续性地改善全国的重要基础设施和关键资源保护形势。

《国家基础设施保护计划》的实施有赖于所有者和运营商自愿提供的重要基础设施和关键资源信息。其中大部分信息为敏感的商业或者安保信息，未经授权而披露或者使用这些信息会对民营公司、经济秩序和公共安全等造成严重破坏。联邦政府对于重要基础设施和关键资源有关的信息负有法定的安全保障义务。通过一系列计划和程序，诸如保护关键基础设施信息（PCII）计划，美国国土安全部以及其他联邦机构可以确保与实现安全相关信息相适应的安全保障。

诸如 1974 年隐私法案规定的要求等，会对《国家基础设施保护计划》中定义的重要基础设施和关键资源保护活动进行规范，其目的是同时实现公民权利和自由的安全和保护。

五、保护重要基础设施和关键资源是美国国土安全使命的重要组成部分

《国家基础设施保护计划》明确提出了重要基础设施和关键资源保护在国土安全使命中的定位。重要基础设施和关键资源保护项目的执行需要各级政府和民营部门的参与、协调和合作。为此，《国家基础设施保护计划》将指导各部门重要基础设施和关键资源计划的结构和内容。《国家基础设施保护计划》将提供一个基本框架，告知各部门特定计划、国家和地方国土安全战略，以及合作伙伴重要基础设施和关键资源保护项目和恢复战略机动事项的研发、应用和更新的进展。

为了达到这个效果，《国家基础设施保护计划》必须补充其他计划，帮助预防和应对恐怖袭击、自然灾害和其他紧急事件，并在此期间提供相应保护、做出响应并从中恢复。联邦政府、州政府、地方政府、部族政府和区域政府的国土安全计划和战略，用于保护其各自管辖区域内的重要基础设施和关键资源。同样，通过制定一系列保护重要基础设施和关键资源的相关计划和项目，重要基础设施和关键资源所有者和运营商已经对于威胁不断增长的环境做出了响应，其中包括商业持续性措施以及恢复和响应措施。在重要基础设施和关键资源合作伙伴之间，可以协调实施《国家基础设施保护计划》，从而确保它不会产生重复性或者高成本的风险管理要求，因为这种要求对于保护重要基础设施和关键资源的强化作用不大。

《国家基础设施保护计划》、国家应急准备指导方针（NPG）以及国家响应框架（NRF）共同为国土安全使命提供了全面的、综合性的途径。《国家基础设施保护计划》建立了全面的风险知情途径，定义了全国重要基础设施和关键资源保护的态势，同时国家响应框架也为国内突发事件管理提供了相应途径。在构建预防能力、保护能力、响应能力和恢复使命能力等方面，国家应急准备指导方针规定了国家的工作重点、法律原则、扮演角色和相应责任。在特定威胁背景或者对于国土安全咨询系统（HSAS）建立的威胁条件做出响应的背景下，增加重要基础设施和关键资源保护措施，可以在《国家基础设施保护计划》稳态保护以及国

家响应框架的事件管理活动之间架设起重要的桥梁。

实施国家响应框架，从而指导国内事件管理活动的综合协调能力。《国家基础设施保护计划》合作伙伴关系和程序会为国家响应框架的重要基础设施和关键资源维度提供基础，从而促进活动范围内的威胁和事件管理，包括事件预防、响应和恢复。通过在评估、规划、培训、练习、许可和技术协助活动中有针对性地发挥能力，贯彻国家应急准备指导方针。实施《国家基础设施保护计划》既是国家的应急准备工作重点，也是实现国家应急准备指导方针中定义的保护能力的基本框架。

六、确保重要基础设施和关键资源保护项目长期有效运行

为了确保重要基础设施和关键资源保护项目能够长期有效开展，《国家基础设施保护计划》提出采取以下机制。

（1）支持国家建立重要基础设施和关键资源保护项目以及相关的投资和活动，确保公众能够清晰理解所有的威胁，并保证受到威胁的国家重要基础设施和关键资源能够及时恢复。

（2）开展教育、培训和科目练习，确保有知识、有技能的专业人士和有经验的组织机构能够在未来承担与《国家基础设施保护计划》相关的责任。

（3）通过新技术的研究、开发与应用，提升重要基础设施和关键资源保护的能力或者降低其运行成本，使重要基础设施和关键资源的合作伙伴能够在有限的预算条件下得到更多的支持。

（4）研发、保障和维护数据系统和模拟系统，在行业部门内外持续实现精确的风险管理，确保为紧急事件的管理做好准备。

（5）按照当前开展的评审和修订的要求，持续提升《国家基础设施保护计划》和相关计划与项目的优势。

七、为重要基础设施和关键资源保护项目提供资源

提出了一个综合性的、风险通报的办法，确立工作重点，确定要求，指引国家重要基础设施和关键资源保护项目的资源支持，按照联邦政府的批准辅助国家、地方、部族和区域团体，支持有关民营部门的活动。在联邦层面，关于重要基础设施和关键资源保护工作重点和要求，美国国土安全部将通过提交国家重要基础设施和关键资源保护年度报告，向总统执行办公室提出相关建议。该报告的编制依据来源于美国国土安全部通过每个部门的特定部门机构（SSA），各州、地方、部族和区域政府协调委员会（SLTTGCC）以及区域财团协调委员会（RCCC）提交的、以国家风险档案和国家工作重点为依据的评估工作重点、要求和相关计划资金信息。通过各州政府、地方政府和部族政府批准而分配联邦资源的过程，使用了类似的途径。美国国土安全部对各州、地方、部族和区域的重要基础设施和关键资源保护工作重点和要求的相关信息进行整合。美国国土安全部使用这些数据，确定了国家保护重要基础设施和关键资源方面的工作重点：优先处理那些在缓解保护计划风险方面最主要的资源。这种风险知情途径还包括在规划过程中涉及民营部门合作伙伴的机制，并且支持重要基础设施和关键资源合作伙伴之间开展合作，从而确定工作重点、界定要求、共享信息并将风险降到最低限度。

《网络空间政策评估》概要

2009 年 5 月 29 日，美国总统奥巴马在白宫公布了由美国国家安全委员会和国土安全委员会负责网络事务的副主管梅利萨• 哈撒韦主持完成的一份网络安全评估报告。报告称来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。奥巴马表示，网络空间以及来自网络空间的威胁都是真实存在的，保护网络基础设施是维护美国国家安全的第一要务。在竞选期间奥巴马就十分强调网络安全对美国的重要性，就任后不久的 2009 年 2 月即要求对美国的网络安全状况展开为期 60 天的全面评估。评估工作于当年 4 月 17 日结束，评估小组将报告提交奥巴马总统审阅。在 17 分钟的致词中，奥巴马总统指出：“我们今天正处于重要的转型时刻，一个历史性的时刻，互连的世界带给我们极大的承诺，也有极大的危险。”他列举了一系列的事实，说明网络对美国国家安全、商业运行和个人利益的重要意义，以及网络安全所带来的重大挑战。他强调，“美国 21 世纪的经济繁荣将依赖于网络安全”，“很明显网络威胁是我们面临的最严重的国家经济和安全挑战之一”，“无论作为一个政府还是一个国家，我们并没有做好应有的准备”，“这种现状不能忍受，我们可以而且必须做得更好”。他宣布：“我的政府将采取新的全面的方式来保护美国的数字基础设施……我承诺这种新做法将从最高层开始：从现在起，我们的数字基础设施——我们每天依赖的网络和计算机——将被视为国家战略资产，它们本该就是。保护这一基础设施将成为国家安全的优先事项。”

奥巴马宣布，为保证实现这一目标，“作为国家安全团队（National Security Staff）的组成部分——白宫将成立一个办公室，由网络安全协调员领导。这是一项非常重要的工作，我将亲自选择这一职位人选。”奥巴马将在五个关键领域开展工作，包括：制定新的全面的网络安全战略，各方面加强合作确保各级组织一致地响应未来网络事件，加强公私伙伴关系，继续投资研发前沿网络安全技术，在全国范围内开展提高网络安全意识的运动。最后，他说：“美国作为发明了互联网、引发了信息革命、改变了世界的国家，将延续在 20 世纪所做的事，并在 21 世纪再次领先。”

一、报告的主要架构

这份评估报告题为“网络空间政策评估：保障可信和强健的信息和通信基础设施（Cyberspace Policy Review：Assuring a Trusted and Resilient Information and Communications Infrastructure）”，全文共 76 页，包括前言、内容提要、简介、正文。正文分 6 章，具体内容如下。

（1）建立最高层的领导。美国通过以下事项来加强对网络安全的领导：设立一名总统的网络安全政策官员和支持架构；审查法律和政策；加强联邦政府在网络安全方面的领导和责任，提升州、地方和部族政府对网络安全的领导。

（2）建立数字国家能力。倡导全国网络安全对话，提高公众的网络安全威胁和风险意识，以及对如何减少威胁和风险的认知。

（3）分担网络安全的责任。讨论改进和扩大联邦政府和民营部门及盟国的伙伴关系的必

要性。

（4）建立有效的信息共享和应急响应机制。美国需要一个全面的框架，促进政府、民营部门和盟国协调地对重要的网络事件做出反应。探讨这样一个框架的组成部分，并建议加强信息共享机制，以提高事件响应能力。

（5）鼓励创新。讨论美国如何利用创新的好处来解决网络安全问题，包括与民营部门一道，确定未来基础设施的性能和安全性目标，将研究和开发与基础设施发展联系起来，更广泛地协调政府、行业和学术研究工作。

（6）行动计划。报告提出了近期和中期行动计划。

二、报告概要

按照美国总统指示，开展为期 60 天的针对美国网络安全政策和结构的全面评估。网络安全政策包括有关网络空间安全和在网络空间中运行的战略、政策和标准，涵盖减少威胁、减少隐患、威慑因素、国际参与、事件响应、网络弹性和恢复的政策和活动，包括计算机网络运行、信息保障、执法、外交、军事和情报任务，这些事项涉及全球信息和通信基础设施的安全和稳定。评估的范围不包括与国家安全或基础设施保障无关的信息和通信政策。政府网络安全专家组成评估小组，搜集的信息来自工业界、学术界、公民自由和隐私社团、州政府、国际合作伙伴、立法和行政部门。报告总结了评估小组的结论，并初步勾勒出迈向可靠的、有弹性的、值得信赖的未来数字基础设施的前进道路。

美国正处于十字路口。全球互连的数字信息和通信基础设施被称为“网络空间”，它构成了现代社会各方面的基础，为国民经济、民用基础设施、公共安全和国家安全提供关键的支持。互联网技术已经以难以想象的方式改变了全球的经济和人们之间的联系方式。然而，网络安全风险也带来一些 21 世纪最严重的经济和国家安全的挑战。构建数字化基础设施是在协同工作性和效率的驱动下发展起来的，安全性考量则不在其中。因此，越来越多的国家和非国家行为体正在损害、盗窃、改变或破坏信息，这将严重威胁美国的系统。与此同时，传统的电信网和互联网继续融合，其他基础设施部门采用互联网并使它成为互相联系的主要手段。美国面临着双重挑战，既要保持促进高效、创新、经济繁荣和自由贸易的环境，也要促进安全、公民自由和隐私权。解决网络空间的战略漏洞，并确保美国和世界充分发挥信息技术革命的潜力是政府的基本责任。

不能允许这种状况继续下去。美国必须向世界表明，自己是以有力领导和远见来认真对待这一挑战的。应当加强领导，由白宫负责以提供指导、协调行动并取得成果。此外，应当加强联邦网络安全领导和问责制。这种方式需要澄清联邦部门和机构与网络安全相关的角色和责任，同时提供政策、法律结构和必要的协调，使它们能够履行其使命。尽管经过过去两年的努力，关键性项目已经启动，在整合不同机构的任务方面也取得了长足进步，但这仍是一个不完整的解决方案。这一问题已超越个别部门和机构的管辖范围，因为尽管每个机构都可以作出各自的贡献，但不是任何一家机构就能单独解决全部问题。

必须立即展开全国性网络安全对话。政府与业界应共同讨论国家可以采取什么方式来解决问题，让美国人民认识到采取行动的必要性。不知道危险多严重，人们是无法认识安全的重要性的。因此，联邦政府应启动国家的公众意识教育。尽管我们还拥有世界上对信息技术公司最有利的环境，但国家应加强相关人才培养以保持美国在全球的竞争水平和领导地位。

仅靠美国政府不能在网络空间安全上获得成功。联邦政府应加强与民营部门合作。公共部门和民营部门的利益是相互交织的，有责任共同确保安全、可靠基础设施。联邦政府可以采取多种方式与民营部门合作。必须不断发展网络安全的政府与民间伙伴关系，明确这种关系的性质，以及各方的角色和责任。联邦政府应审视伙伴关系的现状，优化能力、确定优先事项、有效行动。

国家也需要明确有关网络安全的国际战略，塑造国际环境，与志同道合的国家一起研讨技术标准，以及各方均可接受的地域管辖权、国家主权和使用武力的法律准则。国际规范对于建立安全和繁荣的数字化基础设施起到关键作用。此外，不同国家和地区的法律和惯例（如调查和起诉网络犯罪的法律，数据保存、保护和隐私权，网络防御和应对网络攻击的方法）对于实现安全可靠和有弹性的数字环境是严峻挑战。只有与国际合作伙伴共同努力，美国才能以最佳状态应对这些挑战，加强网络安全，并在数字时代充分获益。

联邦政府有责任保护国家免受网络事件或事故的影响。美国政府有责任保护和捍卫国家，各级政府有责任确保公民的安全和福祉。而大部分支撑政府和个人的数字基础设施由民营部门设计、建设、拥有并运营。美国需要一个全面的框架，以确保联邦、州、地方和部族政府以及民营部门和国际盟友协调一致地响应重大事件。这一框架的执行需要设定报告阈值、可调节的响应、制订灾后恢复计划以及保证计划成功实施的必要的协调、信息共享和事件报告机制。政府应与关键利益相关方一道，设计有效的机制来实现真正的共同运作，整合政府和民营部门的信息通报，为按优先级地降低脆弱性以及事件响应提供支撑。与民营部门合作，必须明确下一代基础设施的性能和安全目标。美国应充分利用技术带来的好处，解决国民经济和国家安全的需要。联邦政策应满足国家安全、保护知识产权的需要，在受到敌人高级攻击的情况下保证基础设施的可用性和不间断性的需要。联邦政府与民营部门和学术界的合作，要明确需要协调的信息和通信基础设施的目标。政府及州、地方的合作，要采取激励措施促进市场为公众提供更安全的产品和服务。政府应探索额外的奖励机制，包括调整法律责任（减少法律责任以换取安全的改善或因安全性差增加法律责任）、补偿、税收优惠，制订新的监管规定和遵守机制。

白宫要引领前进的方向。过去 15 年，美国保障网络安全的手段未能跟上威胁的发展。我们应当向国际和国内社会证明，美国在认真地对待与网络安全相关的问题、政策和活动。这就要求白宫在动员整个国家的各方力量、建议和思想方面发挥领导作用。

三、报告公布的近期和中期行动计划

相关计划见表 2.2。

表 2.2　报告公布的近期和中期行动计划

近期行动计划	
1	任命一名网络安全政策的官员，负责协调全国网络安全的政策和活动；建立一个强大的国家安全委员会的理事会，在网络安全政策官员的指导下，向国家安全委员会和国家经济委员会报告，协调跨部门发展网络安全有关的战略和政策
2	更新的保障信息和通信基础设施的国家战略提交总统批准。这一战略应包括继续评价 CNCI 的工作
3	把网络安全引入总统的关键管理优先事项并制定业绩指标

续表

近期行动计划	
4	在国家安全委员会的网络安全理事会中指定一名负责隐私和公民自由的官员
5	建立跨部门的机制，在政策制定过程中开展网络安全相关问题的法律优先性分析，进行统一的政策指导，明确任务、职责和联邦政府机构在网络安全活动中的地位
6	发起全国性的公众意识和教育运动以促进网络安全
7	明确美国政府对国际网络安全政策框架的立场，加强国际伙伴关系，主动参与网络安全有关的全部活动、政策制定
8	制定网络安全事件响应计划；展开对话，加强政府与民间合作伙伴关系，着眼于汇集资源、调整资源、提供资源，优化各自的贡献和参与
9	协同其他总统行政办公室（EOP），制订研究和发展战略的框架，强调可能改变游戏规则的有潜力的技术，提高数字基础设施的安全性、可靠性、弹性和可信赖性；向研究机构提供网络安全事件数据，便于其开发工具、测试理论并找出可行的解决办法
10	制订网络安全的身份管理的规划和战略，解决隐私和公民自由保护问题，利用隐私增强技术保卫国家
中期行动计划	
1	改进机构间有关网络运行过程中出现的解决流程分歧，这些分歧包括相关的法律解释以及政策与职权的适用性问题
2	使用 OMB 项目评估框架，确保各部门和机构在实现网络安全目标的过程中使用基于绩效的预算编制
3	加大关键教育项目和研发活动的支持力度，确保国家在信息经济时代中拥有持续的竞争力
4	制定扩大和培训劳动力的战略，包括吸引和留住联邦政府中的网络安全专业人才
5	确定最有效率和效果最佳的机制，以获得战略预警、态势感知和告知事件响应的能力。
6	制定一套威胁发生的场景和指标，应用于风险管理决策、恢复规划及确定研发的优先次序
7	制定政府和民营部门之间的协作流程，预防、发现和响应网络事件
8	建立网络安全相关的信息共享机制以解决对隐私和专利信息的关注问题，并使信息共享的各方都能获益
9	开发有关在自然灾害、危机或冲突情况下保持应急通信能力的解决方案，同时确保网络的中立性
10	扩大与主要盟国之间网络事件和隐患信息的共享，寻求双边和多边安排以改善经济和安全利益，同时保护公民自由和隐私权利
11	鼓励学术界和产业界的实验室之间的合作，建立（成果）转移路径和激励机制，以加快研究以及技术开发创新的应用
12	使用基础设施目标和研发框架，明确国家和国际标准机构的目标
13	推行一系列可选的互操作身份管理系统，建立在线交易的信心并加强隐私保密
14	完善政府采购的战略和改善市场激励措施，鼓励采用安全和有弹性的硬件和软件产品、安全创新以及安全管理服务

《实现能源供给系统网络安全路线图》概要

一、能源行业控制系统工作组（ESCSWG）的话

《实现能源供给系统网络安全路线图》制定了改进能源行业网络安全的规划。其中的战略框架呈现了业界、供应商、学术界和政府相关方对能源供给系统安全的愿景，并为在未来十年实现这一愿景确定了目标与里程碑。相关公私部门确定了建设、部署以及管理电力、石油和天然气行业能够抵御攻击的能源供给系统的进程，2011 路线图是这一不懈努力的见证。

2011 路线图是对《2006 年实现能源领域控制系统安全路线图》（*2006 Roadmap to Secure Control Systems in the Energy Sector*）的修订，体现了能源领域对于安全的持续投入（commitment，此处译为投入）。北美洲的供水、交通、通信及其他关键基础设施对能源部门可靠运行的依赖程度日益增加，这使其容易成为高级黑客的攻击目标。鉴于网络威胁具有复杂、多变、持续的特性，且背景雄厚，我们需要更加努力地做到有效预防和响应。

能源行业意识到了这一必要性，80 余家相关企业、组织和部门参与了对路线图的修订。我们要感谢这些参与者，因为其意识到这一努力的重要性，而且愿与我们协力，致力于实现同一愿景。

这一指导性的框架蕴含了参与者的付出与智慧，现在到了我们利用这些资源践行路线图的时候。我们积极鼓励每一个利益相关方把愿景的实现作为己任，确定一个科学的目标或里程碑。研究人员、供应商、学术界、政策制定者以及设施所有者和运营者需要携手迎接我们共同面对的挑战。你们持续的支持与投入是实现这一愿景的关键。

二、执行概要

能源供给系统对北美洲能源基础设施的有效及可靠运行至关重要。我们的生活依赖生产、调动和分配能源相关流程的网络，以及电子元件、通信设备及监测和控制这些流程的人的相互连通。能源供给系统能够为大的分布式网络中的系统操作者和自动控制提供及时、准确的信息，这是可靠而灵活的能源基础设施正常运转的基础。广泛的分布式控制需要多个领域的大量节点和设备之间的连通，这使能源系统和其他赖以运转的基础设施成为意外和蓄意的网络攻击的目标。

对能源行业而言，网络安全是严峻而持续的挑战。能源供给系统遭遇网络威胁会深刻影响国家安全、公共安全和国民经济。民营部门拥有并运营着绝大部分能源行业的关键资产和基础设施，而政府部门需要对国家安全负责，因此，确保能源供给系统免遭网络威胁是政府与民营部门共同的责任。确定一个共同的愿景及实现这一愿景的框架，引导确保能源供给系统安全的公私合作（PPP），显得尤为必要。

三、2011 路线图：肯定进展，明确变化

从 2005 年开始，美国能源部电力传输与能源可靠性局、国土安全部科学和技术分部（the US Department of Homeland Security Science and Technology Directorate）和加拿大自然资源部下设的能源基础设施保护机构一道，促成了《2006 年实现能源领域控制系统安全路线图》以提升能源部门网络安全。2006 路线图确立了一个共同的愿景及战略框架，业界和政府部门以此为指引，研发、部署在遭遇蓄意的网络攻击时核心功能不受影响的控制系统。2006 路线图是控制系统界集体智慧的结晶，资产的所有者和运营者、供应商、国家实验室、行业协会、学术界、政府机构，以及国际社会成员共同参与其中。各种努力与见解汇聚成一个共同的目标，各相关方的知识和资源通过合作与互动得到更好的利用。

2006 路线图的发布开启了国内和国际社会之间在能源领域网络安全问题上的公私合作伙伴关系。路线图的实施目前已取得重大进展。《实现能源供给系统网络安全路线图》是对 2006 路线图的更新与修订，它反映了网络安全技术及其他相关技术的进步，以及行业不断变化的新需求。2011 路线图的更新主要体现在以下几方面。

- **关注范围发生变化。**2011 路线图对能源供给系统有了更广泛的关注，包括控制系统、智能输电网技术以及网络安全与物理安全的连接点（系统元件的物理接入会影响网络安全）。2011 路线图意识到智能技术（如智能电表和相量测量装置）、新的基础设施元件、移动设备使用的增多和新应用正在改变能源信息传播和控制的方式，同时新的安全漏洞也应运而生，并对消费者和能源市场信息保护提出了新要求。
- **以 2006 路线图进展为基础，进一步缩小差距。**2011 路线图确定了新的优先事项：增加政府、研究人员和业界之间的漏洞信息披露；通过创新的伙伴关系充分利用相关方有限的时间与资源；改进对里程碑进展的评估方式；缩小与未来的先进科技之间的差距。尽管 2006 路线图在协调多个公私合作项目、研发投资、互操作性与网络安全标准的形成和采用、高级培训以及加速产品研发等方面建立了稳固的基础，但要应对持续和新兴的挑战，我们仍要做更多的工作。
- **网络威胁日趋高端和复杂。**路线图意识到能源供给系统面对的网络威胁是真实存在的，而且在不断创新，变得愈加复杂和高端。网络攻击者使用逐步创新的技术，利用现代能源供给系统在部件、通信方式及一般操作系统中的漏洞进行渗透并实施蓄意破坏。震网（Stuxnet）蠕虫事件即是网络威胁入侵关键能源基础设施的例子。病毒侵入特定的工业控制系统——可编程逻辑控制器（PLC），修改系统程序，进而对系统元件实施控制。
- **重视安全文化。**路线图意识到增强能源供给系统抵御攻击的能力需要的远不止（对规章的）服从，网络安全文化的渗透是非常必要的。规定和标准仅能够用来提升安全底线。缺乏能够形成并采用适应能源供给系统运行环境的最可行的安全政策、程序和技术的人，便不可能确保能源基础设施的安全与抵御攻击的能力。

四、愿景

到 2020 年，抵御攻击能力强的能源供给系统完成设计、安装，并投入运行，在遭受网络攻击时其核心功能不受影响。

推进实现这一愿景的行动计划，保护关键系统免遭日益复杂与持续的网络攻击，面临着难以克服的技术、商业及制度上的挑战。能源企业早已意识到保护所有的能源资产免受自然、意外和蓄意的损害既不实际也不可行。不过，行业以往的可靠记录也显示，有效的防护需要在预防与快速响应、恢复之间做到平衡。因此，行业确保能源供给系统安全的愿景专注于核心功能，这些功能如若受损，将会导致生命损失、公共危害、环境损害、公众信心丧失或严重的经济损失。这一确定优先顺序的方式（prioritized approach）是能源行业通用的风险管理原则的产物。

五、战略框架

实现能源领域的愿景必须执行如下五方面行动计划。

- **营造安全文化。**鼓励能源行业相关方以多种方式与社会公众展开广泛的对话，探讨安全的意义以及在存在风险的环境下运行可能产生的后果。而安全文化融入可靠性实践，将确保安全风险管理方法得到周期性的回顾并不断接受新的质疑，进而确认既定的安全控制仍在发挥作用且能源供给系统的变化或新的威胁没有削弱其有效性。执行这一行动计划将有助于行业实现如下目标：网络安全实践是反思性实践（reflexive practice），期待能源领域所有相关方予以践行。
- **评估和监测风险。**评估和监测风险使企业能够全面了解其当前的安全态势，进而对不断演进的网络威胁、安全漏洞和风险进行持续的评估，并做出响应。执行这一行动计划将有助于行业实现如下目标：针对所有能源供给系统体系结构水平和跨信息-物理领域的持续的安全状况监测，被能源行业的资产所有者和运营者广泛采用。
- **形成并实施新的防护措施以降低风险。**当安全风险（包含安全漏洞和新的威胁）被识别或预见的时候，这一行动计划要求形成并实施新的防护措施，把系统风险降低到可接受的水平。这些安全举措将会被下一代能源供给系统采用，针对旧有系统的安全措施也会设计出来。执行这一行动计划将有助于行业实现如下目标：下一代能源供给系统的体系结构能够提供深层防御，其使用的部件具有互操作性、可扩展性，且在遭遇降级的条件下能够继续运行。
- **网络安全事故处理。**绝对的安全并不存在，任何系统在新的威胁面前都显得十分脆弱。当积极主动的防护措施没能阻止网络安全事件发生时，检测、补救、修复能够将事故的影响最小化。事故后的分析和取证则能够使能源行业相关方从中吸取教训。执行这一行动计划将有助于行业实现如下目标：网络安全事件发生时，能源领域相关方能够将其影响减轻，快速恢复系统的正常运行，从中吸取教训并对能源供给系统环境中的新变化有所认知。
- **推动网络安全状况的持续改进。**长期内，积极主动地改进能源供给系统安全状况需要强大而持续的资源投入、清晰的激励机制，以及相关方之间的密切合作。能源行业的合作提供了提升行业抵御攻击能力的资源与激励举措。执行这一行动计划将有助于行业实现如下目标：业界、学术界与政府合作，推动网络安全状况的持续改进。

这些行动计划与清晰的里程碑一起，构成了战略框架的核心。它将协调公私部门的努力并结合新的项目提升能源供给系统安全。

六、主要挑战

能源行业实现战略框架的里程碑面临许多挑战。如下挑战不分优先顺序，每一个对实现行业愿景都很关键。然而，行业必须应对的挑战并不止这些。

尽管自 2006 路线图实施以来，能源企业评估和监测网络安全态势的能力已有所改进，但应对日益尖端的网络威胁的实时解决办法依旧欠缺。这些威胁难以预测，且行业形成和部署对策的能力跟不上其变化的步伐。网络威胁动态化的特性使度量的一致性和风险度量工具的创新变得复杂化。由于现有设备和体系结构固有的局限，升级旧有系统通常需要替代技术来确保必要的安全能力，否则安全升级会导致系统性能退化。具内置安全和端到端安全性的新体系结构的研发及在整个能源行业的部署需要多学科的努力和重要的资源投入，并要花费数年的时间。关于网络攻击及其后果、吸取的经验教训等信息通常不在攻击发生的部门之外共享。网络安全问题、它们可能带来的后果，以及对适用于能源供给系统的解决办法的需求，也不为能源供给界之外所了解。

网络安全相关的商业投资也极为复杂。网络威胁快速变化且不可预测，其可能产生的后果也很难论证，这为量化环境风险带来了困难。

规定的变化及推陈出新导致的监管不确定性也会给民营部门网络安全投资带来风险。

美国政府问责办公室（GAO）承认，目前联邦和州的监管环境形成的安全文化就是公用事业部门对网络安全规定的（被动）服从，而不是（积极主动）去实现全面、有效的网络安全。

七、路线图的实施

实施这一路线图需要政府、业界、学术界、研究人员、供应商、其他解决方案提供者，以及资产所有者和运营者的共同努力。这些利益相关方发挥其专长，致力于改进能源供给系统当下和未来的安全。行业组织和政府机构能够提供必要的协调、领导和投资，处理主要的障碍和分歧。政府实验室和大学的研究人员在帮助行业探索长期的解决方案并研发工具软件方面发挥关键作用。资产所有者和运营者承担确保系统安全、适时增加投资和贯彻防护措施的主要责任。软件和硬件供应商、承包商、IT 和电信服务提供商，以及适用于能源供给系统的产品和服务的技术设计者，共同为上述努力提供支撑。

评估进展对最终实现愿景至关重要。进展取决于遍及北美地区的利益相关方为实现这一共同目标所采取的行动。人工确认并记录相关方的进展极为耗时，且需要集中的资源。为解决这个问题，ESCSWG 鼓励相关各方使用 ieRoadmap 网站记录他们为提升网络安全采取的举措。通过 ieRoadmap 网站，相关方能够平衡（align）资源，合作形成战略性和策略性的方法，将其付诸实践以实现路线图的里程碑，并于每年定期评估、交流进展。ESCSWG 将帮助协调和评估能源领域实现路线图愿景的（总体）进展。

《全球供应链安全国家战略》概要

近年来，国际贸易已经并且不断成为美国和全球经济增长的强大引擎，通信技术进步和贸易障碍以及产品成本的减少有助于全球资本市场的扩张并带来新的经济机会。支持这一贸易的全球供应链系统对于美国经济是十分必要的，并且它是一项关键的全球资产。

通过全球供应链安全国家战略，我们围绕美国政府的相关政策来强化全球供应链，从而保护美国人民的福利和利益，并且保障我们国家的经济繁荣。在该战略中我们关注的是运输、邮政、运输途径、资产和基础设施的全球性网络，借助这一网络商品从生产点到达最终的消费者，以及支持通信基础设施和系统。本战略包含以下两个目标。

目标 1：促进商品的有效和安全运转。该战略的第一个目标是在保护和保障供应链免受剥削的同时促进及时、有效的合法商业流程，并且降低供应链的脆弱性。为了实现这一目标，我们将在商品于供应链中流转的时候加强其完整性。通过现代化供应链基础设施和流程寻求贸易最大化时，我们还将在流程早期理解和解决风险，并且加强物理基础设施、运输工具和信息资产的安全。

目标 2：建立一个弹性供应链。该战略的第二个目标是建立一个有准备、能够抵抗不断进化的风险和危害并且能够从毁坏状态快速恢复的弹性供应链。为了实现这一目标，我们将优先考虑努力减轻系统漏洞并且在毁坏之后改善和重新建立商业流的计划。

我们遵循的方法由以下指导原则启发而来。

（1）激励作用。在美国政府以及国家、地方、部族和领土政府、私人机构与国际社会中，汇聚并且激励努力。

（2）管理供应链风险。定义、评估和利用分层防御优先努力管理风险，并根据安全和操作环境的变化调节安全状况。

为支持本战略，在联邦层面，我们将升级威胁和风险评估，整合项目和资源，并引入政府、私有部门和国际社会的利益相关方。联合各方的目的是寻求具体建议来报告和指导本战略的协同实施。

一、简介

全球供应链供应食物、药品、能源和维持我们生活的产品。许多不同实体对全球供应链的运作要么负责，要么依赖于它，包括监管者、执法部门、公共部门采购者、民营企业，以及其他国内外合作伙伴。全球供应链系统依赖于运输基础设施和途径、信息技术、计算机网络和能源网络组成的一个互连大网络。它们相互依赖促进经济活动的同时，也有利于在广阔地理区域内或者产业内传播风险（起因于本地或者区域性的干扰）。

美国政府，协同其他国家、地区、部族、国际社会和私有部门相关利益方，已采取多项措施来强化全球供应链。这些措施包括法律要求的实施和许多具有特定安全关注点的战略努力。这一战略包含并且建立在那些事先努力的基础之上。

二、战略目标

我们力求建立和保护一个能够及时在本国市场以及世界各地安全可靠地运转货物，并且支持创新和繁荣的全球供应链系统。我们必须保护现有系统的连贯性，同时通过实施能够强化系统并且促进合法全球贸易运转的有效和划算的措施，构建新的未来。

目标 1：促进商品安全和有效运转

当保护和保障供应链，防止剥削并降低其受到破坏的脆弱性时，我们都在共享促进及时、有效的合法贸易流的集体利益。通过将安全和效率链接于一个目标下，美国政府旨在强调安全是实现供应链系统高效率和正常运转的一项必要元素。

为了实现我们的目标，美国政府将力求：

（1）尽早解决威胁以促进合法的贸易流程。通过将安全进程整合到供应链运作中，我们能够确定关注事项并且力求尽可能快地解决它们。

（2）提高核实和检验的能力，以鉴定货物，并且阻止货运通过该系统被连累或误导。

（3）加强基础设施和运输工具的安全以保护供应链和关键节点，对货运、基础设施、运输工具等进行访问控制。

（4）通过实现供应链基础设施和流程的现代化，扩大合法贸易流以满足未来的市场机会；开发新的机制来促进低风险货运；简化贸易流程；并且改善激励措施来鼓励利益相关方合作。

目标 2：建立弹性供应链

集成的供应链高效并且成本低，但是也容易受冲击，诸如从局部事件迅速升级为更大范围的中断的影响。我们将力求建立一个准备好并能够抵挡进化中的风险和危害，并且能从中断中快速恢复的弹性系统。增加的弹性和灵活性、动态能力将提高国家承受冲击、拯救生命的能力，并且减少中断的总体影响。

为了实现我们的目标，美国政府将力求：

（1）通过利用风险管理原则，在潜在事件之前降低系统供应链中断的脆弱性，以识别和保护关键资产、基础设施和支持系统；积极推进可持续操作过程的实施和对于相关资产的适当冗余。

（2）通过开发与实施国家和全球指南、标准、政策和程序，推动贸易恢复政策和实务，为潜在破坏下货物运转的协调恢复做好准备。

三、战略方法

我们实现这些目标的方法是由一系列原则报告和指导的，它们反映了我们作为一个国家的价值观、信仰和优先考虑的事。这些定义我们方法的原则包括我们在联邦政府内外激励作用，以及通过把我们的努力集中在那些引起最显著改进或风险降低上，有效管理风险的能力。

该战略集中于世界范围网络上的交通运输、邮政和运输途径、资产及基础设施等组件，借助这些组件货物运转到达最终消费者。这包括制造、装配、整理、包装、运输、仓储以及支持的通信基础设施和系统。

四、激励作用

为了迎接挑战，强化供应链，我们必须推动在各级政府、私有部门以及其他关键利益相

关方之间采取经过整合的共同行动。为实现我们的战略愿景，我们将力求：

（1）通过寻找更智能和更省钱的方式来解决安全威胁并且最大化来自美国各地政府的资源和专业知识，集中联邦政府的努力。通过发展类似要求、简化流程以及增强信息共享实践，我们将努力改善贯穿联邦政府的措施。

（2）在强化供应链上，促进一个全民参与的方法以平衡由国家、地方、部族和地方政府扮演的重要角色。我们将通过授权这些利益相关方为这一使命作出贡献，以此来管理它们的活动与联邦政府之间的裂缝。这将同时发展一种互惠和责任共享的文化。

（3）通过加强我们与国际社会和外国那些具有关键供应链角色和职责的利益相关方之间的协调，立足全球。全球供应链超越国界和联邦管辖。认识到这一点，我们将与国际社会共同寻求制定和实施全球标准，加强检测、封锁和信息共享能力，并且促进端到端的供应链安全。

五、管理供应链风险

全球供应链正遭受着不断演进的风险。作为一个国家，我们的竞争力取决于管理关于供应链的物理基础设施风险，以确保货物、能源、人民以及信息从一个地方移动到另一个地方的能力。为了管理风险，我们将：

（1）理解并解决那些企图引入有害产品或材料的系统开发和由恶意攻击、事故或自然灾害引发的中断所带来的供应链脆弱性。我们将重点关注那些最能够带给美国公民伤害或者影响供应链系统功能的威胁。

（2）利用防御层来保护自己免受各种各样的传统和不对称的威胁。这些防御层包括：情报和信息分析，技术的适当使用，我们的法律、法规和政策，适当的培训和训练有素的人员，以及有效的伙伴关系。

（3）调整我们的安全形势以适应不断发展的威胁。我们将努力促进一个动态和灵活的风险管理方式，优先行动以解决那些潜在影响力最大的风险。我们必须同时建立一个可以评估新兴威胁并相应地变更行动优先顺序的环境。

六、前进的道路

该战略将在发布后立即实施。在短期内，我们将把关注点放在战略形成阶段所确定的优先行动领域。这些（行动领域）包括：

（1）联合横跨美国政府的联邦活动以实现战略目标。

（2）通过更新的评估改善我们对全球供应链所带来的威胁和风险的理解力。

（3）先进技术的研究、开发、测试和评估工作，旨在提高我们保障空中、陆地和海上环境货运的能力。

（4）识别能够作为关键基础设施弹性的最佳实践模型的基础设施项目。

（5）寻求机会将全球供应链的弹性目标和宗旨吸收进联邦基础设施投资计划和项目评估过程。

（6）促进必要的立法，以支持联邦政府部门和机构实施该战略。

（7）与产业和外国政府开发定制化的解决方案，加速具体的满足特定标准并且被认为是

低风险的供应链的合法商业流。

（8）联合联邦各机构的可信赖贸易项目要求。我们将考虑由联合或交叉任命的联邦团队所指导的标准化应用程序、增强的信息共享协议以及安全审计的潜能。

除上述联邦政府努力以外，我们还将积极参与国内和国际合作，制定具体建议，并且绘制出实现它们的过程图。我们已经建立了一个正式的流程来征求反馈意见，这些反馈来自有任务在身或者对全球供应链有兴趣的利益相关方。

各部门和机构将通过助理向总统提交国土安全和反恐怖主义以及关于该战略发布后一年内实施情况的汇总报告。该报告将详细介绍上面确定的每一优先行动领域的进展情况。它也将包括对未来在扩大服务范围过程中采取进一步行动的一些建议。

七、结论

我们所追求的全球供应链将通过在国内外迅速、安全、可信地运转货物和服务支持创新和繁荣。本战略对合作伙伴来说是宣言，对于对手来说是警告，我们不断努力强化这一重要系统。我们不仅要在过去努力的坚实基础上建立本系统，并且要放眼我们正在努力创造的未来。因此，我们的战略具有承上启下和开拓意义。自然灾害的威胁依然存在，并且全球供应链及其组成部分对于恐怖主义袭击和恶意开发来说依然是具有吸引力的目标。然而公民和国家的安全是最受关注的，我们必须通过对世界保持企业开放，努力促进美国未来经济的增长和国际竞争力。

《提升美国关键基础设施网络安全的框架规范》摘译

美国的国家和经济安全离不开关键基础设施的可靠性。伴随着关键基础设施的复杂性和关联性的增加，信息安全威胁使得国家的安全、经济和公众的安全以及人民的健康面临着风险。如同信誉和金融风险一样，信息安全风险对组织机构造成了影响，它不仅增加了消耗、影响了组织机构效益，而且伤害了组织机构的创新能力，导致顾客流失。

为了更好地应对这些风险，总统于 2013 年 2 月 12 日签署了第 13636 号行政令——《增强关键基础设施信息安全》。该文件是“美国政府为提高国家关键基础设施的安全与可靠性，保障安全的网络环境，并在提高生产效率、创新能力与经济繁荣的同时，保证生产的安全稳定，保护组织机构商业机密、隐私及公民自由的政策文件”，该行政令要求自发形成一种基于风险的信息安全框架规范——以一系列的标准和最佳惯例来帮助组织机构管理信息安全风险。该框架规范由政府和私人组织机构合作创建，用最通俗的语言阐述了在基于商业需求的前提下，用最经济有效的方法来应对和管理信息安全风险，该框架规范并不会增加另外的商业监管要求。

该框架规范利用商业驱动的方式来指导信息安全操作，并且将信息安全风险作为组织机构风险管理程序的一部分。该框架规范由三部分组成：框架规范核心（core）、框架规范适用标准（profiles）、框架规范实施层面。框架规范核心是一系列的信息安全操作、实现效果以及关键基础设施领域常见的信息参考文献的集合，它能提供详细的指导用来建立组织机构适用标准。通过使用框架规范适用标准，组织机构能将其信息安全操作与商业需求、风险容忍和资源结合起来。框架规范实施层面能帮助组织机构认识和理解其管理信息安全风险的方法的特点。

该行政令也要求框架规范包含相应的方法，使得关键基础设施组织机构在设计信息安全操作时能保护个人隐私和公民自由。尽管生产程序和需求不同，该框架规范仍然能将个人隐私和公众自由融合到综合信息安全规划中。

该框架规范适用于任何组织机构，不论其规模、信息安全风险程度和信息安全复杂度如何，组织机构都可以采用风险管理机制和最佳惯例来提升关键基础设施的安全和恢复力。该框架规范为组织机构提供了最新的多种安全策略，汇总了在工业上有效的标准、指导和惯例。另外，由于其参考了全球的信息安全意识标准，所以该框架规范可以为国外公司提供一个国际合作模型用来加强关键基础设施的信息安全。

该框架规范并不是万能的用以管理关键基础设施信息安全的方法，组织机构会继续面临一些特殊的风险——不同的威胁、不同的薄弱点、不同的风险容忍度，从而导致其在实现框架规范时会存在差异。组织机构可以根据关键服务的分布来决定其操作，也可以对投资进行优先分级以最大化投资产生的效益。最后，该框架规范的目的是降低和更好地管理信息安全风险。

该框架规范并非一成不变，当接收到工业应用中的反馈之后，它将会继续进行更新和改进。伴随着该框架规范的投入应用，未来的版本中会提供相应的学习课程。当关键基础设施

所有者和操作者处于动态和挑战性的环境中，面临着新的威胁、风险和解决方案时，该措施能够满足他们的需求。

使用该自愿性质的框架规范的下一步工作是提高美国关键基础设施的信息安全——向私人组织机构提供指导，从而提高国家关键基础设施融合的信息安全。

一、框架规范介绍

美国的国家和经济安全依赖于关键基础设施的可靠运行。为了强化这些基础设施的恢复力，奥巴马总统于 2013 年 2 月 12 日颁布了题为《增强关键基础设施网络安全》的第 13636 号行政令[1]。在该行政令中，总统呼吁开发一种自愿性的网络安全框架规范（以下简称 “框架规范”），以便提供“优先化、可靠性、可重复、基于性能、成本有效性手段”来管理提供关键基础设施服务程序中直接涉及的流程、信息和系统方面的网络安全风险。产业中联合开发的这种框架规范，能够为组织机构管理网络安全风险提供相应指导。

在该行政令中，关键基础设施被定义为“那些对国家至关重要的系统和资产，不论是物理的还是虚拟的，所谓至关重要是指一旦该系统或资产的能力丧失或遭到破坏，就会削弱国防安全、国家经济安全、公众健康或安全或者这些重要方面的任意组合”。由于所面临的内部和外部威胁压力不断增加，负责操作关键基础设施的组织机构需要采取连续性、重复性的途径来识别、评估和管理网络安全风险。无论组织机构的规模如何、威胁暴露程度如何或者今天的网络安全复杂程度怎样，采取这种途径都是十分必要的。

关键基础设施的相关组织机构可以分为公共和私有的所有者和运营商，以及那些保障国家设施安全的组织机构。关键基础设施的功能部分的实现必须由信息技术（IT）和工业控制系统（ICS）[2]来支持。IT和ICS的技术、彼此间的交流以及互连导致了潜在的脆弱点的改变和扩大，增加了运行的潜在风险。例如，当在提供关键服务和支持商业决策程序中越来越多地使用工业控制系统以及运行工业控制系统产生的数据时，我们应当考虑到网络安全事件给组织机构的商业、资产、个人健康和安全以及环境带来的潜在影响。为了更好地管理这些网络安全风险，我们需要更加清楚地理解：组织机构在使用信息技术和工业控制系统程序中涉及的商业驱动因素和安全注意事项。因为各个组织机构的风险都有其独特性，伴随着信息技术和工业控制系统的应用，为实现框架规范所描述的结果而采取的工具和方法各有不同。

由于认识到隐私保护和公民自由在打造更牢固的公众信任程序中所发挥的重要作用，总统所颁布的行政令要求：框架规范应当包括关键基础设施组织机构在开展网络安全活动程序中为了保护个人隐私和公民自由而采取的方法途径。许多组织机构已经出台相关措施来应对隐私和公民自由问题。这种方法途径旨在补充这些措施，并提供相关指导，以促进按照组织机构网络安全风险管理方法来开展隐私风险管理。隐私保护和网络安全的融合，可以使得组织机构通过提高消费者信心、共享更为标准化的信息以及简化法律机制内的运营程序等方法获益。

---

[1] 总统第 13636 号行政令，增强关键基础设施网络安全，DCPD-201300091，2013 年 2 月 12 日。请参考以下网址：http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf。

[2] 美国国土安全部关键基础设施计划提供了部门列表及其相关关键功能和价值链条。请参考以下网址：http://www.dhs.gov/critical-infrastructure-sectors。

为了确保可扩展性，并实现技术创新目的，该框架规范不对技术发展做任何干预。该框架规范依赖于各种不同的现有标准、指导方针和惯例，从而使得关键基础设施供应商能够具备恢复能力。通过依赖产业所开发、管理和更新的这些全球化标准、指导方针和惯例，实现框架规范目标所用工具和方法会跨越国界，识别出全球范围内的网络安全风险，并且随着技术进步和商业要求的发展而不断进化。现有和新兴标准的应用能够促进经济不断升级，并且驱动有效产品、服务和惯例的发展，从而满足公认的市场需求。市场竞争也会促进这些技术和惯例的快速扩散，从而实现利益相关方在这些领域内的诸多收益。

通过建立这些标准、指导方针和惯例，该框架规范提供了一种通用的分类和机制，具体如下。

（1）描述当前的信息安全情形。

（2）描述信息安全的目标状态。

（3）确定连续和可重复的程序的范围并对其进行优先提升。

（4）在实现目标的过程中评估其进展。

（5）与内部和外部的利益相关方就有关信息安全风险进行沟通。

该框架规范用于补充，但是不会取代组织机构的风险管理程序和网络安全计划。组织机构可以使用其现有程序，充分发挥该框架规范的作用，以识别出潜在的机遇，从而强化和传达其网络安全风险管理方法，同时也满足产业惯例要求。另外，当前还未制定网络安全计划的组织机构也可以使用该框架规范作为参考来制定其计划。

该框架规范并不针对任何具体产业，因此，它所规定的任何普遍分类标准、指导方针和惯例，也不会针对任何具体国家。位于美国境外的组织机构也可以使用该框架规范，以强化其自身的网络安全努力，并且该框架规范也可以为关键基础设施网络安全方面进行的国际合作开发共同语言作出贡献。

（一）框架规范概述

该框架规范采用了基于风险的方法来进行信息安全风险的管理，其由三部分组成：框架规范核心、框架规范实施层面和框架规范适用标准。每部分都用来加固商业驱动和信息安全操作的联系。

1. 框架规范核心

其由信息安全操作、期望的结果、关键基础设施领域内常见的应用参考文献组成。该核心提供了工业标准、指导方针和惯例的方式，该方式使得组织机构内部的行政层面到执行/操作层面都能进行信息安全的操作和输出结果的交流。该框架规范核心包含五个并行和连续的功能——识别、保护、检测、响应、恢复。当一起考虑这些功能时，它能提供基于管理信息安全风险生命周期的高层面、战略性的视角。

该框架规范核心不仅为各种功能提供了不同的分类和子分类，并且匹配了相应的参考信息案例文献，如现有的标准、指导方针和惯例。

2. 框架规范实施层面（以下简称“层面”）

该层面提供了一个环境，使组织机构认识到信息安全风险和处理程序，从而管理信息安全风险。层面描述了组织机构安全风险管理惯例程序表现出来的基于框架规范特征的分级

（如风险和威胁感知、重复性、自适应）。层面将组织机构的惯例进行了分级，从局部的（层面 1）到自适应的（层面 4）。这些层面反映了从非正式、被动响应到快速、风险感知的处理这个连续的程序。在层面选择程序中，组织机构应当考虑到其当前的风险管理惯例、威胁环境、法律法规、管理需求、商业/任务客体以及组织机构约束。

3. 框架规范适用标准（以下简称“适用标准”）

该适用标准体现了组织机构从框架规范里选择了分类和子分类后产生的结果。适用标准可以理解成将框架规范核心中的标准、指导方针、惯例应用到特定的场景后产生的结果的特征。通过对比“当前”适用标准（“目前”状态）和“目标”适用标准（“将要到达”的状态），它可以用来识别出能提高信息安全态势（Posture）的机会。为了建立一个适用标准，组织机构应当检阅所有的分类和子分类，考虑商业驱动和风险评估，最后选择最重要的分类。组织机构可以在面临风险时增加分类和子分类。“当前”适用标准可以用于支持优先次序和测量对比，在向“目标”适用标准转换时，会面临着其他的商业需求。适用标准可以用来自我评估和在组织机构内部或组织机构之间进行交流。

（二）风险管理和信息安全框架规范

风险管理是指由风险识别、评估和应对组成的一个持续的程序。为了实现风险管理，组织机构应当了解事故发生的可能性以及造成的后果。有了这些信息，组织机构可以决定它们的风险接受水平以便提供相应的服务，并且将其表达成它们的风险容忍能力。

了解了其风险容忍能力之后，组织机构可以优先考虑信息安全操作，从而使得组织机构能对信息安全开支做出明确的确定。风险管理计划的实施给组织机构提供了量化和沟通调整自身网络安全计划的能力。组织机构可以采用不同的方式来处理风险，如减轻风险、转移风险、避免风险或者接受风险，方式的采用取决于风险对关键服务造成的潜在的影响程度。

该框架规范通过使用风险管理流程，使得组织机构能获取信息安全信息和对其进行优先的处理选择。该框架规范支持循环的风险评估和商业驱动的验证，从而帮助组织机构选择信息安全操作的最终目标状态，并通过期望输出来体现最终目标状态。因此，该框架规范能使组织机构动态选择和直接提升信息安全风险管理计划，以便应用于信息技术和工业控制系统环境。

此框架规范适用于提供灵活的、基于风险的实施途径，兼容广泛的网络安全风险管理程序。网络安全风险管理程序实例包括国际标准化组织（ISO）31000:2009[1]、国际标准化组织/国际电工委员会（ISO/IEC）27005:2011[2]，美国国家标准与技术研究所（NIST）专业出

[1] 国际标准化组织，风险管理-基本原则和指导方针，ISO 31000:2009，2009 年。请参考以下网址：http://www.iso.org/iso/home/standards/iso31000.htm。

[2] 国际标准化组织/国际电工委员会，信息技术-安全技巧-信息安全风险管理，ISO/ICE 27005:2011，2011 年。请参考以下网址：http://www.iso.org/iso/catalogue_detail?csnumber=56742。

版（SP）800-39[1]、电力子领域网络安全风险管理程序（RMP）指导方针[2]。

（三）文件概述

本文件的其他内容如下。

第 2 节描述了该框架规范的构成：框架规范核心、层面和适用标准。

第 3 节阐明了如何使用该框架规范。

附录 A 以表格形式阐释了该框架规范核心：功能、分类、子分类和信息参考。

附录 B 包括所选术语的词汇表。

附录 C 列出了本文件中所使用的首字母缩略词。

二、基本框架规范

该框架规范提供了一种通用语言，用于理解、管理和表达内部和外部的网络安全风险。它可以用于帮助识别和优先化降低网络风险的措施，也是调整政策、商业和技术途径以管理相关风险的一种工具。它可以用于管理整个组织机构内部的网络安全风险，也可以聚焦组织机构内提供的关键服务。不同类型的实体机构（包括协调机构部门、社团和组织机构等），可以使用该框架规范来达到不同的目的，包括创建普遍的适用标准。

（一）框架规范核心

该框架规范核心提供了一系列的操作和指导方针的参考案例，以便获取特殊的信息安全输出结果。该核心不是需要执行的操作清单。它提供了行业中关键的信息安全输出结果，以便对管理信息安全风险有所帮助。该核心由四部分组成：功能定义、分类、子分类、信息参考文献，如图 2.3 所示。

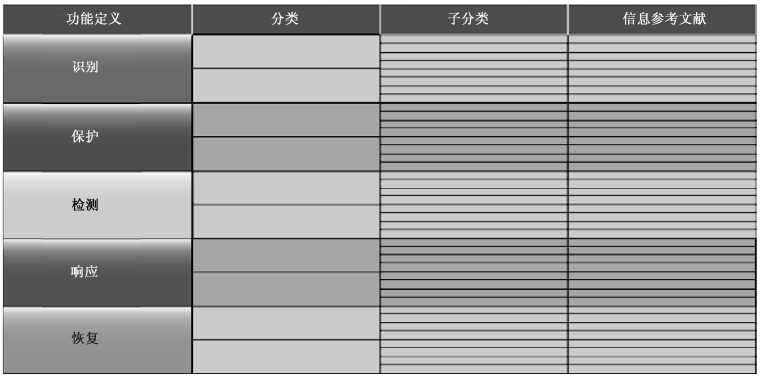

图 2.3　框架规范核心结构

[1] 联合任务组过渡计划，管理信息安全风险：组织机构、任务和信息系统观察， 美国国家标准与技术研究所专业出版 800-39，2011 年 3 月。请参考以下网址：http://csrc.nist.gov/publications/ nistpubs/800-39/SP800-39-final.pdf。

[2] 美国能源部，电力子领域网络安全风险管理程序，美国能源部/OE-0003，2012 年 5 月。请参考以下网址：http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf。

框架规范核心元素定义如下。

功能定义：功能是指将基本的网络安全操作以最高层面体现出来，这些功能为识别、保护、检测、响应和恢复。它通过组织机构信息的方式帮助组织机构来表现其网络安全风险的管理、风险管理决策、应对威胁，通过学习以往的操作来提升性能。该功能还能配合已有的事件管理方法，将应用于网络安全的投资产生的影响显现出来。例如，对实时响应和恢复操作的计算和执行支持上的投资，会降低对所提供服务的影响。

分类：分类是指将功能细分成与纲领性需求和特殊操作密切关联的网络安全结果的分组。例如，分类包含“资产管理”、“接入控制”和“检测程序”。

子分类：子分类是将分类再细分成基于技术和管理操作的特殊的输出结果。它提供了一个不够详尽的结果用来支持每个分类都能达到其期望的结果。例如，子分类包含“对外部信息系统进行编目”、“静止数据需要保护”、“来自检测系统的通知需要研究”。

信息参考文献：这些文献由关键基础设施领域内常用的标准、指导方针、惯例组成，其描述了与每个子分类相关输出结果相关的实现方案。这些文献是说明性的，并非是巨细无遗的。它们在框架规范开发程序[1]中的跨职能的指导方案中经常被引用。

框架规范核心的五个功能并不是串行的或者是为了产生一个静态的期望结果，它们可以并行和连续地产生操作方法，以便应对动态的网络安全风险。

以下对这五种功能进行定义。

（1）识别：使组织机构能了解系统、资产、数据和功能所存在的网络安全风险。基于识别功能的操作是建立在对框架规范有效利用的基础之上的。了解商业环境、支持关键功能的资源、相关联的网络安全风险，可以使组织机构能聚焦和优先化其工作方向，该方向与风险管理策略和商业需求一致。例如，该功能的输出结果分类为资产管理、商业环境、治理手段、风险评估以及风险管理机制。

（2）保护：建立或提升适当的保护机制以保护关键基础设备服务的传送。 保护功能提供了限制和控制潜在的网络安全事件影响的能力。该功能的输出结果分类包含：接入控制、意识和培训、数据安全、信息保护程序和步骤、维护以及保护技术。

（3）检测：建立或提升适当的操作，用来识别网络安全事件的发生。检测功能可以实时发现网络安全事件。该功能的输出结果分类包含：异常和事件、连续性的安全监视、检测程序。

（4）响应：建立或提升适当的操作，用来应对检测到的网络安全事件。响应功能能提供控制潜在的网络安全事件影响的能力。该功能的输出结果分类包含：响应计划、交流、分析、缓解以及提升。

（5）恢复：建立或提升适当的操作，以便用来保存恢复计划、还原由于网络安全事件所损害的能力或服务。恢复功能能够提供及时恢复到正常操作的能力，以便减少网络安全事件的影响。该功能的输出结果分类包含：恢复计划、系统提升、交流。

---

[1] 在制定框架规范程序中，美国国家标准与技术研究所通过信息要求输入、网络安全框架研讨会和利益相关方参与等方式采集了信息参考文献纲要。此纲要包括协助实施的相关标准、指导方针和惯例。此纲要的目的不是要变成一种详尽列表，只是基于初始利益相关方输入而形成的起点。通过以下网址：http://www.nist.gov/cyberframework/，可以参考此纲要和其他的支持性材料。

（二）框架规范实施层面

框架规范实施层面提供了相应的标准环境，通过对比该标准，组织机构可以识别网络安全风险以及处理程序，以便对风险进行管理。该层面从局部（第一层面）到自适应（第四层面），描述了在网络安全风险管理惯例中严谨性和复杂性逐步增加的程度，网络安全风险管理基于商业需求并将其融合到组织机构中全部风险管理的习惯做法中。风险管理需要考虑网络安全方向，包含了个人隐私以及公众自由，与网络安全风险管理和潜在的风险响应之间的融合程度。

层面选择程序考虑了组织机构的现有风险管理惯例、威胁环境、法律和监管要求、商业/任务目标以及组织机构的约束条件。组织机构应当确定其所需层面，确保所选水平能够满足组织目标，并且具有实施可行性，从而将关键资产和资源的网络安全风险降低到组织机构可以接受的水平。组织机构应当考虑充分利用联邦政府部门和机构以及信息共享和分析中心（ISAC）颁布的外部指导方针、现有的成熟模型或者可以帮助确定其所需层面的其他资源。

当组织机构被识别为第一层面（局部）时，鼓励其向第二层面或者更高层面升级，层面并不能代表成熟度。当这种变化能够降低网络安全风险并且证实具有成本有效性时，鼓励其向更高层面升级。框架规范的成功实施，应当基于组织机构目标适用标准中描述的实现结果，而非确定的层面。

层面定义如下。

1. 第一层面：局部

（1）风险管理程序：组织机构的网络安全风险管理的习惯做法是非正式的，风险管理处于一种时有时无的状态。网络安全操作的优先级没有直接考虑到组织机构的风险客体、威胁的环境、商业/任务的需求。

（2）综合风险管理计划：对目前的网络安全风险意识有限，尚未建立整个组织机构范围内的网络安全风险管理机制。组织机构在处理网络安全风险时是不规则的、就事论事的，处理方式采用的信息来源于外部资源。组织机构也许不具有将网络安全信息与别的组织机构共享的能力或计划。

（3）外部参与：组织机构不具有与其他组织机构进行协调或合作的程序计划。

2. 第二层面：风险感知

（1）风险管理程序：风险管理惯例是指已被管理层批准，但没有被确立为全组织机构范围的策略。网络安全操作优先级的选择来源于组织机构的风险客体、威胁的环境、商业/任务需求。

（2）综合风险管理计划：在组织机构层对网络安全风险有意识，但尚未建立组织机构范围内的网络安全风险管理机制。基于风险告知、管理层批准的程序和规划已经被定义和应用，另外已分配足够的资源去实现网络安全目标。网络安全信息在组织机构内部非正式共享。

（3）外部参与：组织机构知道自己在大体系中的地位和角色，但没有与外界进行接触和共享并确定其具体的功能。

3. 第三层面：可重复性

（1）风险管理程序：该组织机构的风险管理方法被批准并作为一项政策。网络安全方案

定期在风险管理程序应用结果的基础上进行更新，或者随商业/任务需求、威胁、技术背景的改变而改变。

（2）综合风险管理计划：存在于全组织机构范围内的网络安全风险管理方案。基于风险告知的政策、处理程序、规划已被确定、有目的实现、定期更新。一致性方法有效应对风险的变化。具有相应知识和技能的人员被用来实现其指定的任务和职责。

（3）外部参与：组织机构了解其依赖关系和合作伙伴，并且从这些合作伙伴那里接收相应的信息用来进行合作，在组织机构内部针对安全事件制定基于风险的管理决策。

4. 第四层面：自适应

（1）风险管理程序：基于课程学习、从以往和当前的网络安全操作程序中获取的预测指标，组织机构自适应地建立了网络安全实现方案。通过不断地改善先进的网络安全技术和惯例的程序，组织机构能积极适应经常变化的信息安全背景，能及时应对不断发展和复杂的威胁。

（2）综合风险管理计划：存在于全组织机构范围内的信息安全风险管理方案，该方案利用风险告知策略、处理流程、规划来应对潜在的信息安全事件。信息安全风险管理是组织机构文化的一部分，并且通过对以往操作的意识、其他资源共享的信息、对当前系统和网络内连续操作的认识不停进化。

（3）外部参与：组织机构能管理风险，能主动与合作者分享信息以保证发送和读取精确的、最新的信息，从而能在信息安全事件发生前提升信息安全能力。

（三）框架规范适用标准

该框架规范适用标准是功能、分类、子分类和商业需求、风险容忍、组织机构的资源的结合。框架规范使组织机构建立一个降低信息安全风险的路线图，该路线图可以很好地实现组织机构和各部门之间目标一致，考虑到法律法规要求和行业内最佳实现方案，以及响应风险管理程序的优先级设置。鉴于一些组织机构的复杂性，它们可以选择多重适用标准，实现不同组件的统一并了解其独有的需求。

该框架规范适用标准可以描述当前的状态或者特殊的网络安全操作所期望的状态。当前适用标准体现了当前获得的信息安全的成果。目标适用标准显示了需要实现的信息安全风险管理目标的最终输出结果。适用标准支持商业任务需求，有助于组织机构内部和组织机构之间进行风险知识的交流。 该框架规范文件并不会指定适用标准模板，允许在实施程序中灵活处理。

比较不同的适用标准（如当前适用标准和目标适用标准）可以揭示差距。组织机构认识到这些差距有助于实现信息安全风险管理目标。处理这些差距的措施对路线图有所帮助。缩小差距的措施的优先级由组织机构的商业需求和风险管理程序所驱动。基于风险的方法使得组织机构对现有的资源进行评估，以成本高效和优先方式来实现信息安全目标。

（四）框架规范实施协调

图 2.4 描述了在组织机构内部不同层面间的信息和决策流，这些层面分为以下三种：

- 行政层；

- 商业/程序层；
- 实施/操作层。

行政层将任务的优先级别、可提供的资源、总体风险容忍的信息传送给商业/程序层；商业/程序层将这些信息输入风险管理程序中，然后与实施/操作层合作进行商业需求的传输以及创建一个适用标准；实施/操作层将适用标准执行进展传送到商业/程序层；商业/程序层利用这些信息进行影响评估；商业/程序层管理人员将影响评估的结果传送给行政层，以便行政层了解全组织机构所有的风险管理程序。

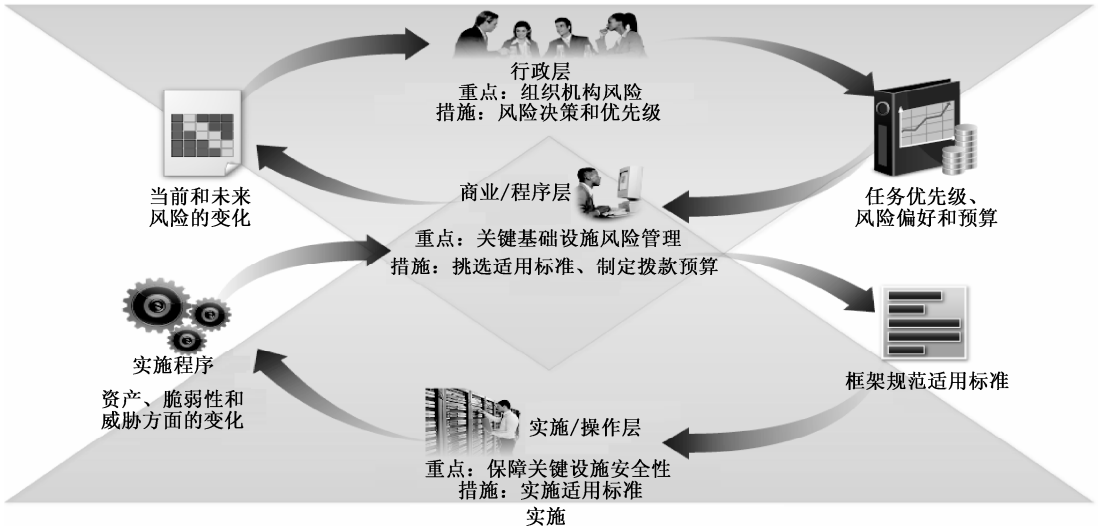

图 2.4　组织机构内部信息和决策流

三、如何使用框架规范

组织机构可以使用该框架规范作为系统程序中的一个重要部分，可以识别、评估、管理信息安全风险。该框架规范并不是用来取代现有的处理程序，组织机构可以将当前的处理程序覆盖到框架规范中去，以便发现当前信息安全风险处理流程的不足之处和建立一个提升性能的路线图。利用该框架规范作为信息安全风险管理工具，组织机构可以确定那些对关键服务传送至关重要的操作和优先处理开支以便最大化投资的影响。

该框架规范是对现有的商业和信息安全操作的补充，可以用来创建一个新的信息安全计划或者创建一个可以提升现有计划的策略。该框架规范将网络安全需求传达给商业伙伴以及顾客，并且有助于识别组织机构的信息安全方案的差距。它同样提供了一系列的注意事项和处理程序，这些程序为个人隐私和公众自由对信息安全计划造成的影响。

（一）信息安全惯例方案基本情况

该框架规范可用来比较组织机构内当前信息安全操作与框架规范核心内容的概况。通过建立一个当前的适用标准，组织机构可以检测它已获得的成果达到了何种程度，这些成果在核心中的分类和子分类中已描述清楚且与五种高级功能（识别、保护、检测、响应、恢复）一致。组织机构将会发现已经达到其想要的结果，因此，该信息安全管理与已知的风险相平

衡。相反，组织机构可能判定其有机会（或者需要）提升信息安全能力。组织机构可以使用这些信息来设立一个操作计划加固已有的信息安全惯例方案和降低信息安全风险。组织机构也许会发现它在获取特定的结果时投入过多。组织机构可以使用这些信息来调整资源的优先级以加强其他信息安全的惯例。

假如不需要取代风险管理程序，这五个高水平的功能将会为高级管理人员和其他人提供一个简洁的方式来提炼信息安全风险的基本概念，使他们能够评估识别风险的管理方式。该框架规范同样能帮助组织机构回答基本的问题，如“我们如何做”，然后以一种明确的方式来加强信息安全的惯例。

（二）制定或者改进信息安全计划

接下来介绍组织机构如何使用框架规范来创建一个新的信息安全计划或者改进已有的计划，这些步骤也许会迭代以提高信息安全。

步骤 1：确定优先级和范围。组织机构应当识别出其商业/任务目标和高层防的组织机构的优先事项。有了这些信息，组织机构可以制定信息安全实施的战略决策，并确定支持选择的商业线或处理程序的系统和资产的范围。该框架规范适合于支持组织机构内部不同的商业线或处理程序，而该组织机构具有不同的商业需求和相关的风险容忍能力。

步骤 2：确定方向。一旦基于商业线和处理流程的信息安全计划的范围被确定了，组织机构就可以识别出相应的系统和资产、调整相应需求和整体的风险方法。组织机构也能识别出系统和资产面临的威胁和存在的薄弱点。

步骤 3：创建当前的适用标准。组织机构可以建立当前的适用标准，该适用标准根据框架规范核心中的分类和子分类的输出结果来确定当前需要取得的结果。

步骤 4：开展风险评估。该项操作可以将组织机构的整体风险管理程序或以前的风险评估作为指导。组织机构能对操作环境进行分析，以便得到信息安全事件发生的概率及其对组织机构造成的影响。对于组织机构来说，将新出现的风险、威胁和脆弱的数据变成易于理解的安全事件发生的概率及影响，这项工作是很重要的。

步骤 5：创建一个目标适用标准。组织机构创建的目标适用标准，聚焦于利用框架规范的分类和子分类对组织机构需要得到的信息安全输出结果进行评估和描述。组织机构也许会建立额外的分类或子分类来应对特殊的组织机构风险。组织机构也许会考虑组织机构以外的利益相关方的需求和影响来创建目标适用标准，如部门实体、顾客、商业伙伴。

步骤 6：确定、分析以及对差距进行优先分类。组织机构将当前的适用标准与目标适用标准进行对比以确定差距，接下来，组织机构根据商业驱动、成本/效益分析、对目标适用标准中的输出结果的理解来建立一个优先操作次序。然后组织机构确定应对这些差距所必需的资源。采用这种方式来使用适用标准可以使组织机构做出有关信息安全操作的明智决定，支持风险管理，进行具有成本效益、有针对目标的改进。

步骤 7：实施行动计划。组织机构需要决定哪些操作被用来应对差距，如果这些操作存在的话，那么就需要在先前的步骤中区别开来。接下来依靠目标适用标准对当前的信息安全惯例操作进行监视。为了进行更加深入的指导，框架规范应当对有关分类和子分类的事例参考文献进行识别。但是，组织机构应根据其部门特性、更好的工作需求来确定标准、指导方针、惯例。

一个组织机构可以重复上述步骤，如需要连续进行评估和提升信息安全能力。例如，组织机构会发现其通过重复性的确定方向操作来提升风险评估的质量。

此外，组织机构通过迭代更新当前适用标准来监视当前的处理程序，随后将当前适用标准与目标适用标准进行比较。组织机构也可以利用这些步骤来统一其信息安全计划和期望框架规范实施层面。

（三）与利益相关方交流信息安全需求

利益相关方可以利用框架规范提供的简明方式进行交流，而交流的内容为关键基础设施必不可少的服务。例如：

（1）一个组织机构可以利用目标适用标准来表达其信息安全风险管理的需求，并将该需求传递给外界的服务提供商（如一个云计算提供商所导出的数据）。

（2）一个组织机构可以通过当前适用标准来表达其信息安全状态，以便记录下结果或与收集的需求进行对比。

（3）一个关键基础设施的业主或操作员可以利用目标适用标准传送需求分类或子分类的方式来确定其需要关联的外界合作伙伴。

（4）一个关键基础设施部门可以设立一个目标适用标准，利用其内容作为一个初始基线资料，以建立自己的定制目标适用标准。

（四）在重新建立或修改参考文献时抓住机会

新的或修改的标准、指导方针、惯例可以帮助组织机构找到机遇，而附加的信息参考文献可以帮助组织机构面对新出现的需求。组织机构在实施已有的分类或者建立新的分类时，也许会发现只有极少数与相应操作有关的信息参考文献。为了解决这一问题，组织机构应当与技术带头人合作，参与标准的起草、制定与协调，整合标准、指导方针与惯例。

（五）保护个人隐私和公众自由的方法

这部分主要描述了行政命令由于信息安全操作而对个人隐私和公众自由造成的影响的处理方法。 这种方法旨在设定一整套注意事项和程序，因为隐私和公民自由的含义可能因领域和时间的不同而不同，组织机构可以通过更为广泛的技术实施程序来处理这些注意事项和程序。但是，并不是网络安全计划中的所有活动都能产生这些注意事项。还要制定技术隐私标准、指导方针和其他最佳惯例，才能支撑改进型的技术实施方案。

当个人信息被使用、收集、处理、维护或者在信息安全操作时被泄露时，就会产生个人隐私与公众自由的问题。以下是一些可能需要考虑到个人隐私和公众自由的操作：导致个人信息被过度采集或过度保留的信息安全操作；与信息安全操作无关的个人信息的泄露和使用；导致拒绝服务或类似潜在不利影响的信息安全缓解操作，包括一些对表达和关联自由造成影响的事件检测或监管操作。

组织机构和政府部门应当直接负责由信息安全操作导致的公众自由的保护。拥有或操作关键基础设施的组织机构和政府部门应当遵照隐私法律、法规和宪法的要求开展信息安全活动。

对于保护隐私，组织机构应当考虑哪些措施是适当的。信息安全计划应当包含隐私原则，

包括：在信息安全事件中，有关个人信息材料的数据应当减少收集、泄露和保留；限制基于信息收集的外部信息安全操作活动；某些特定的信息安全操作透明；在对个人信息进行操作时应当获取当事人的同意或对当事人进行补偿；数据质量、完整性、机密性；责任与审查。

组织机构可以将以下程序和活动看成解决以上提及的隐私和公民自由问题的有效途径。

1. 网络安全任务管理

（1）组织机构对于网络风险的评估以及潜在的风险响应，应当考虑网络安全计划中的隐私问题。

（2）负责网络安全有关隐私问题的个人应当向相应的管理部门报备，并且要经过适当培训。

（3）将相关程序部署到位，保证网络安全活动能够符合适用隐私法律、法规和宪法要求。

（4）将相关程序部署到位，评估前述组织机构措施和控制方法的落实情况。

2. 个人访问系统或资产之前进行识别认证的方法

采取措施以识别和解决访问控制措施的隐私问题，它们涉及个人信息的收集、泄露和使用。

3. 推广和培训措施

信息安全工作人员的培训和推广活动中包括来源于组织机构隐私策略的使用信息。

为组织机构提供信息安全服务的服务提供商都会被告知组织机构适用的隐私策略。

4. 异常行为检测和系统资产监控

在组织机构异常检测和信息安全监视程序中进行隐私审查。

5. 响应操作，包含信息共享和其他缓解措施

评估和应对是否、什么时间、以何种方式、多大范围内个人信息被组织机构外界进行共享，该操作为安全信息共享活动的一部分。

对组织机构的信息安全缓解措施进行隐私审查。

第三章　美国网络安全战略译文

战略（计划）篇

信息系统保护国家计划（V1.0）

一、总统的话

在不足一代人的时间内，信息革命和计算机在社会各个层面的引入已经改变了我们的经济运行方式、保障国家安全的方式以及日常生活的组织方式。不管是在家中打开电视机、登上飞机，还是因为亲人生病而寻求帮助，我们都要依赖于一个或者多个复杂的计算机驱动系统。同样，我们最为复杂的国防系统所依赖的商业、通信和运输业也都需要用到计算机控制。未来，计算机技术将继续为美国人民创造新的机会。

这个充满希望的时代也充斥着危险。所有受计算机驱动的系统都容易遭到入侵和破坏。我们的重要经济部门或者政府机构的计算机一旦受到合力攻击，将会产生灾难性的后果。

我们知道，这种威胁是事实存在的。曾几何时，我们的对手只是依赖于炸弹和子弹；如今，一台笔记本电脑就是敌对分子和恐怖分子可能利用的武器，从而给我们造成巨大的破坏。如果想继续享用信息时代所带来的种种益处，捍卫我们的安全，保卫我们的经济成果，就必须保护我们重要的计算机控制系统免受攻击。

这就是在审阅了总统委员会关于关键基础设施保护的报告后，我在 1998 年 5 月发布第 63 号总统令的主要原因。这个总统令要求行政部门评估国家关键基础设施的计算机的易受攻击性，这些基础设施包括：信息和通信系统、能源部门、银行和金融业、运输业、水利系统、应急服务部门、公共安全，以及负责联邦、州和地方政府职能不间断地运转的领导机构。该总统令着重强调了要保护政府自身的关键资产免受计算机攻击，同时还强调了对其缺陷进行修正的必要性，目的是使政府成为信息安全的典范。

总统令还要求联邦政府制定保卫国家免受计算机破坏的详细计划。

信息系统保护国家计划是一系列更为复杂的工作的第一步。随着我们对正在出现的威胁和易受攻击性的认识不断深入，我们的计算机保护计划将得到持续发展和更新。它向我们展示了一种综合性的解决方案，为我们的经济建设、国家安全、公共健康和安全中的关键部门

提供了保护措施。

为成功实施这项计划，政府和私人业主必须齐心协力，结成前所未有的合作关系。只有举国上下团结应战，我们才能达到目标。因此，我已经要求内阁成员与操作关键基础设施的私人工业和公共服务的代表进行密切的合作。我们不能指望仅靠政府法令就能实现我们的目标，各部门必须自己决定保护其关键系统所必需的方法、步骤和标准。作为合作关系中的一方，联邦政府要随时准备提供帮助。

当然联邦政府自身也有重要任务，其中包括：在计算机安全领域内开展研究，培养青年科学家来帮助保护我们的联邦计算机系统，协助民营部门制定其保护信息技术的措施。

当我们推进计划时，所有美国人都应该知道，增强我们的计算机保护措施不能也绝不会以牺牲公民的自由为代价。我们绝不能危害我们要极力保护的自由。

我在计划里设定的各项任务时间表是内容宏大的，需要我们国家领导阶层的支持、紧密的政府与民间的合作以及必要的法律和财政拨款。然而，这是一项我们现在就必须着手启动的重要任务，只有如此，我们才能享用信息时代提供给我们的众多机会，并为下世纪的繁荣和发展建立我们必需的安全基础。

比尔·克林顿

二、国家协调员的话

这个计划是世界上首次由一国政府实施、用来设计其国家计算机空间保护方案的尝试性活动。

（一）美国的新依赖和美国的新威胁

与其他国家相比，美国对其计算机空间的依赖性更强。对国家的计算机空间的攻击可以破坏我们的输电线路、电话网络、运输系统以及金融机构。所有这些部门都依赖涉及计算机系统的控制网络。

在下一场战争中，敌人的目标将是美国的基础设施，敌人的新武器将是针对我们的关键网络和系统的计算机攻击。我们知道有一些政府正在发展这种能力。

因此，我们需要重新设计国家的信息基础设施结构。在过去十年里，我国信息基础设施的建设非常迅速，但没有对安全给予足够的重视，并没有考虑到富有经验的敌人可能会攻击它。现在我们则必须有所行动，进行保护、防止攻击或者减少已经存在的易受攻击性。

总统已经要求制定一个计算机空间保护计划，而且这个计划要在 2000 年 12 月前初步生效，到 2003 年 5 月完成。为了达到这个目标，我们必须迅速行动，我们有很多事情要做。

（二）真正的公私合作——非指令性解决方案

总统要求联邦政府成为计算机系统安全的典范，但现在事实并非如此。国防部在建立安全系统方面做得非常好，但同样关键的民用机构通常没有充分地得到对计算机系统的保护。这个计划提出了国防部和其他联邦政府部门要采取的很多后续步骤。

民营业主的基础设施至少也是计算机系统攻击的目标。在现代社会，关键的工业和公用事业已经成为各种冲突中的破坏目标。美国的国力就在于私人所拥有和运作的很多关键基础

设施和产业。

私人拥有的计算机网络正处在扫描和渗透之下，某种情况下还成为破坏、偷窃、间谍活动和攻击的目标。虽然总统和国会能够命令联邦网络实现安全化，但他们不能也不应该为民营部门的系统指定解决方案。

因此，在现阶段，这个计划对私人网络的安全和保护不做具体安排，只是为其建议一个公共框架。一些私人组织已经决定联合起来保护它们的计算机网络。

当它们开展这些活动时，联邦政府就能够而且一定会帮助它们。然而政府不会指定任何解决方案，也不会出台任何条例和规定。政府更不会侵害公民自由、隐私权或私有信息。

这是第一版的国家计划。为了进一步完善它，我们真诚地征求大家对这个计划的意见。一旦民营部门实体做出了更进一步的降低易受攻击性和增强保护措施的决定和计划，这些进步将会在后续计划版本中得以反映。

（三）解决方案的各个组成部门——首先是经过训练的人员

这个计划将为我们的计算机空间建立防御体系，它依赖的是全新的安全标准、多层次的防卫技术、全新的研究以及对人才的培训。其中最为急需但最难以达到和实现的就是具有受过训练的计算机科学家和信息中心专家核心。

一个世纪以前，为了应用电力，美国迅速实现了电力布线，国家马上为这个新的经济产业培训出了电气学家和电气工程师。但是，迄今为止，面对刚刚出现的以信息技术为基础的新经济，美国还没有训练出运作、改善和保护其安全的信息技术专家。本计划将提出一系列的步骤来刺激高等教育，培养出美国在这一领域内迫切需要的人才。

继我们的计算机防卫计划之后，我们将推出第二项计划。后者将集中关注政府如何与国家的基础设施部门合作来确保那些重要服务的可靠性和安全性，使其免受大规模的破坏。这个即将推出的计划主要依赖于各家公司和组织的投入——这些公司和组织中各种各样的复杂网络正在为美国人民提供着经济福利、健康、保险和安全。

（四）人民和国会

这个计划是联邦政府中很多人士广泛工作的结果。以他们的名义，我们把这个计划提供给全国人民以及各位众议员，希望举国努力来完善这一计划，保卫我们的计算机空间，保卫依赖于这个计算机空间的各方力量和我们的人民。

理查德·克拉克

安全基础设施保护和反恐怖主义国家协调员

三、执行摘要

（一）介绍

在这个世纪之交，联邦政府和私人业主齐心协力，使得我们平稳过渡到了 2000 年。为了避免千年虫可能造成的信息系统故障和服务崩溃，我们曾做了广泛的准备工作，现在这些准备工作已经初见成效，关键系统保持了连续运行，没有出现任何重大故障。这些事情说明，

必须记住我们处在一个动态的环境中，计算机攻击的性质和我们为保护信息系统所做的准备将始终处于变化之中。随着全新的保护措施的发展及投入使用，那些试图攻击我们的人也会变得更加具有创新性。现在联邦政府正在评估千年虫防御的经验，用来决定未来防卫计算机攻击的可持续性措施的各个相关方面。

这个文件是世界上第一次由国家政府实施、用来设计国家计算机空间保护方案的尝试性活动。总统曾经在第 63 号总统令中对其出台做了指示。把它指定为“版本 1.0”，表明了这个计划还处于发展的初期，还有很多工作要继续。

该计划的第一个版本主要关注联邦政府为保护国家以计算机为基础的关键基础设施在国内所做的工作。后续版本将包括 PDD63 中所考虑的更为广泛的内容，包括工业界、州及地方政府在保护私人所属的基础设施时（单独或与政府合作）所起的作用，以及对物理基础设施的保护和关键基础设施保护中关于国际事务的思索。为了完善我们的计划，我们广泛征求了工业界、国会、州和地方政府以及普通民众的意见，在后续版本中将囊括这些意见。

关键基础设施是指那些对国家十分重要的物理性和基于计算机的系统和资产，它们一旦受损或者被破坏，将会对国家安全、国家经济安全以及/或者国家公众健康及保健产生破坏性的冲击。

PDD63 要求国家计划为关键基础设施保护的目标、原则和长期计划制定出优先级次序，在初期阶段，国家计划的重心主要在于当前联邦政府的计算机安全和信息技术需求。

（二）威胁

在美国，控制政府和工业关键网络的计算机系统——防卫设施、高压输电线、银行、政府机构、电信系统以及运输系统——每天都会受到成千上万次的攻击尝试。

这些攻击尝试中有的以失败告终，有的却取得了成功。有的人获得了“系统管理员的身份”，下载了密码，安装了探针以复制交易信息，或者插入了后门以方便其以后进入。

有的攻击者就像驾车兜风的偷车贼，把犯罪当成一件乐事。有的攻击者则是为了从事间谍活动、偷窃、报复性破坏和勒索。还有的攻击者可能是为了收集情报、预先侦查或者创造未来攻击的能力。这些作恶者种类甚多，从青少年到小偷，从有组织的犯罪团体到恐怖分子，还有潜在的军事敌对力量以及情报机构。这些威胁的严重性在最近几年不断增加。

我们还知道一些外国政府正在为对付美国的计算机网络而发展强大的攻击能力。

美国在基础服务上对计算机网络的依赖性越来越强，以至于很容易受到攻击。然而我们在如此紧密地依赖计算机网络的同时却很少注意保护它。水、电、气、通信（语音和数据）、铁路、航空和其他关键设施都在巨大的信息系统网络中直接受到计算机的控制。

在未来的危机中，犯罪团伙、恐怖分子集团、敌对国家会制造经济破坏、混乱和死亡，并通过攻击这些关键性的网络来降低我们的防卫响应能力。中央情报局局长乔治·特纳德曾证实：“这种威胁是很现实的。”

（三）保护隐私和公民自由

基础设施保护的目标要在与公民全面的自由权利保持一致的前提下得到实现。事实上，一些基础设施保护计划提高了网络环境中数据和通信的安全级别，从而能对个人隐私和其他的公民自由权产生积极的影响。

联邦政府有义务保护计算机用户的个人信息。政府之所以成为这些信息的信托对象，是因为美国公民相信他们的关键性个人信息在这些系统中得到了安全的保存。

联邦政府意识到，用以保护信息和系统的参数如果使用不当，将会在无意中损害公民的自由。即使初衷是好的，但如果保护入侵的技术使用得太广泛，也可能会波及一些正当的行动。尤其在那些个人权利很敏感或有争议的地方，我们有必要认真地考虑与此相关的一切问题。

在权限、安全标准和认可协议等方面，法律并不总能提供清楚的指导方针。计算机入侵事件经常给我们提出复杂的法律和司法问题。

因此，政府保护基础设施和公民自由权利的诸多项目都需要仔细计划、分析，并要求所有受影响的实体的参与。

这份国家计划中所有的提议都完全符合现行的法律以及人们对隐私保护的期望；同时，计划的某些部分将促使大家更关注个人隐私被损害以换取基础设施保障这一问题。

既要使基础设施得到保护，也要与公民的自由权利相一致，寻找这样的解决方案是个动态的过程，必须包括政府和民营业主团体的参与。这个过程中，必须意识到现有司法制度的复杂性和重要性，还要建立新的项目以防止意外后果的出现。

在这样的背景之下，几项重要原则可以作为国家计划中用于分析其项目的出发点：与隐私权团体协商以定义可行的解决方案；对计划各项目进行严格而彻底的法律审查；遵循已有的法令和规则；政府必须作出榜样；评审各种隐私解决方案；与国会合作；与国家科学院合作；致力于教育与意识的培训；遵循由信息基础设施任务组隐私工作组制定的隐私原则。

（四）计划概览

该计划的目标是在 2000 年 12 月之前使关键信息系统的防卫性能初步运行，在 2003 年 5 月完全运转。系统防卫性能投入运行后，美国将有能力确保“这些关键功能遭到的任何破坏或操纵被控制在跨时短、频率低、可控、地域上可隔离以及对美国的利益损害最小的规模上”。

为了实现克林顿总统所确定的在 2003 年建立起对国家关键基础设施的完全防卫这一最终目标，这个计划的现行版本围绕以下三项目标进行设计。

准备和防范：减小对关键信息网络进行成功攻击的可能性，建立面对类似攻击仍能保持有效运转的基础设施。

检测和响应：实时地确定和评估攻击，对攻击进行控制，收到攻击后迅速恢复和重建。

建立牢固的根基：我们应该为我们的国家培养相关人员、建立相关组织、完善法律和传统惯例，使我们能更好地针对关键信息网络遭到的攻击进行准备、防范以及检测和响应。

为此，该计划的 1.0 版本提出了 10 项计划。包括：

（1）准备和防范。

计划 1：确认关键基础设施资产及互依赖性，评估其脆弱性。

（2）检测和响应。

计划 2：检测攻击和非法入侵。

计划 3：开发稳健的情报和执法功能，与现行法律保持一致。

计划 4：实时共享攻击警报和信息。

计划 5：建立响应、重建和恢复能力。

（3）建立牢固的根基。

计划 6：为支持计划 1～5，加强研究和开发。

计划 7：培训和雇用足够数量的信息安全专家。

计划 8：推广，使美国人民知晓提高计算机安全的必要性。

计划 9：采用立法和拨款手段支持计划 1～8。

计划 10：在计划的各步骤和各部分中，要全面保护美国公民的自由权、隐私权和私有数据。

本摘要下面的部分将具体描述每项计划及相应的时间表。

这份计划已经过总统的批准，将为联邦各机构和部门准备各自的预算提供全面的方针和指导，但它不是一个用于决定预算的文件。各机构保护其信息系统时的资金拨款决定将遵照常规的 OMB（关系和预算办公室）预算步骤做出。

计划 1：确认关键基础设施资产及互依赖性，评估其脆弱性。

“首先，了解自己。”

计划 1 要求政府和民营部门确立关键信息网络的重要资产、互依赖性和脆弱性，然后制定并实施实际可行的方案去修复其脆弱性，同时不断地更新评估和修复工作。

对关键信息系统和计算机网络防卫做准备的第一个必要步骤就是全面评估关键基础设施系统的资产、互依赖性和脆弱性。我们将不断估计我们的对手对我们的关键基础设施进行破坏的能力。但同时，我们的保护工作必须建立在确认关键基础设施并评估其脆弱性的基础之上。

我们还没有意识到共享的基础设施系统的互依赖性。经验显示，大多数——如果不是全部的话——信息系统很容易遭受入侵，特别是有内部人员帮助时。虽然有了防火墙和口令系统的广泛应用，但非法入侵还是经常发生。一些防火墙功能有限或没有经常升级，而且有的技术还可以绕过防火墙。用户经常使用太简单的口令，或者很少定期更换它们。一些可以通过公开渠道获得的软件程序就能破解口令。用户还有可能无意中使用了黑客给他们的软件，这些软件在这个系统中秘密安装了后门。还有一些使用者可能违规安装了未授权的调制解调器——这样他们就可以在家里工作——结果在无意中为他人进入网络开了方便之门。

确定计算机网络资产和脆弱性的主要工作计划如下。

- 基于机构/部门之间国家安全和日常任务的区别，确认最关键的资产。
- 分析政府内部或者政府和民营部门之间的共享互操作性。
- 基于对关键资产的确认和共享互操作性的分析，系统管理员、操作者、安全专家和 CIO 对网络脆弱性进行评估。
- 由受过相关训练的外部专家对这些工作进行评价。

信息系统安全操作建议和标准能够帮助各组织确认和发现脆弱性。虽然很多工作都已经做过了，但信息系统安全中的操作建议和标准的公共可接受框架仍处在形成阶段。联邦政府、民营部门和标准制定团体的紧密合作可以制定出更加适用和可接受的指导方针，各组织确认脆弱性时可以此为参考，并对修正脆弱性定出有限级次顺序。在这些指导方针广泛使用以前，联邦政府将努力强化其自身的信息系统安全操作建议和标准。

限于技术和资金，所有的脆弱性不可能同时被立即修正。在 3～5 年的时间内，基于关

键资产的确认和互依赖性分析，政府机构和民营部门将给这些修正工作排出优先级顺序。详细的资金要求必须由首席基础设施保障官（CIAO）、首席信息官（CIO）和首席财政官（CFO）共同做出，然后由内阁成员或者首席执行官（CEO）和公司董事会采纳。

术语“一个互联网年”通常指三个月。信息技术发展得如此迅速，以至于一年前采用的项目和计划与现行的新技术可能没有多少联系。随着网络的变化，新的脆弱性又会被引入。随着黑客对系统的不断揣摩，他们又会发现先前不为人所知的脆弱性。因此，我们要持续不断地审查新的脆弱性、新的保护措施以及新的操作建议和标准。我们要对技术变化导致的个别安全环节所表现出的脆弱性给予足够的重视。

由于关键资产、共享互操作性和脆弱性的评估会给敌人提供攻击方法的蓝图，这些评估本身也要得到保护。要保证有合适的保护措施，包括可能的立法手段等（见计划 9）。

联邦政府机构要持续地进行这种意义深远的风险和脆弱性评估，开发现实可行的多年度修正计划。对这些评估和计划要做到持续更新。同样，信息系统安全中的操作建议和标准也要有相应的更新。联邦各部——PDD63 在它们中指定了基础设施部门联络官——将和民营部门共同合作，促进类似的评估和修正工作。计划 1 时间表见表 3.1。

表 3.1　计划 1 时间表

联邦各部加强计算机安全的行动		
阶段	行动	目标时间
1.1	联邦一期机构完成最初的脆弱性评估，制定修正计划。ERT 将分析其报告	已完成（1999 年 2 月）
1.2	联邦二期机构完成最初的脆弱性评估，制定修正计划。ERT 将分析其报告	已完成（1999 年 5 月）
1.3	联邦各机构向 OMB 提交一份多年度的脆弱性修正计划，同时提交 2001 年的预算，以后每年如此。ERT 将和各部合作执行其修正计划	已完成（1999 年 6 月）
1.4	CIO 委员会将成立关于联邦信息系统安全操作建议的一个跨部门工作组，致力于确定、协调以及巩固正在开展中的政府安全操作建议制定活动。工作组将指导每年向 CIO 委员会做出安全操作建议的推荐报告。工作组还可以向 NIST 修订的《联邦信息处理标准》提出建议。NSA 和 NIST 将依据 1987 年的《计算机安全法案》继续制定操作建议	已完成（1999 年 11 月）
1.5	联邦政府将开发一个实验性框架及数据库，还包含若干实例，以获取并存储确保关键信息资产安全的操作	已完成（2000 年 1 月）
1.6	通过参照《PKI 组件最小互操作性规范（MI SPC）》，使联邦 PKI 用户和外部 PKI 成员用户之间的证书和 CRL 轮廓得到增强，以满足 MISPCv2 的主要管理要求；建立联邦 CA，加强 PKI 组件的互操作性基准，满足 MISPCv2 保密性要求	2000 年 2 月
1.7	联邦政府完成关键物理基础设施保护计划的第一版	2000 年 6 月
1.8	关于操作建议的跨机构工作组将至少每年一次向 CIO 委员会提出有关所推荐的新的或修改过的操作建议的书面报告。CIO 委员会将发布每一份报告，同时附上评论	2000 年 6 月
1.9	国防部关键资产拥有单位、国防基础设施部门的关键基础设施保障官以及设施和装备基地将确认其关键资产并执行初步的脆弱性评估。另外，DI 部门关键基础设施保障官将执行部门级的脆弱性评价，确认关键的部门资产	2000 年 8 月

续表

联邦各部加强计算机安全的行动		
阶段	行动	目标时间
1.10	各国防基础设施部门和国防部关键资产所有单位将建立初步的方法和步骤，用于物理安全脆弱性评估、技术援助、认证和鉴定、认识安全事件及计算机事件	2000 年 8 月
1.11	联邦政府制定用来确认关键基础设施资产和互依赖性的方法	2000 年 9 月
1.12	国防部将完成其关键计算机系统物理保护的检验和评审，包括保密和非保密网络	2000 年 9 月
1.13	联邦各机构将确保软件补丁的实时安装以及其他计算机系统脆弱性修正措施的实施。必要时，OMB 将监督这一过程的执行情况	2000 年
1.14	民营部门信息共享和分析中心将为会员公司开发一套用于评估和修正项目的推荐方针	2000 年
1.15	国防部将更新其对关键基础设施保护程序的检查，针对同关键计算机网络相关的基础设施的主要脆弱性而确定并推荐修正意见	2000 年
1.16	民营部门信息共享和分析中心将评估各民营部门和工业界共有的脆弱性	2000 年
1.17	国防部将建立适当的组织机构来确认和修正脆弱性、开发并配置入侵检测系统、开展重要的创新研究和开发项目	2000 年 11 月
1.18	国防部关键资产所有单位以及部门各关键基础设施保障官将提供修正计划并为修正计划提供资源。另外，国防部设施和装备基地将向部门关键基础设施保障官提供设施装备级的修复计划和资源	2000 年 11 月
1.19	国防部关键基础设施部门 CIAO 将监控响应活动，协调相关部门的缓和及重建活动，并为国家军事指挥中心（NMCC）提供支持	2000 年 11 月
1.20	DI 部门关键基础设施保障官将执行部门级的修正措施，并整合和协调各部门内部资产级的修正计划	2000 年 12 月
1.21	联邦机构已经完成了信息系统脆弱性评估，采用了多年度资金计划来修正这些脆弱性，创造了用于持续更新的系统。每一关键行业的民营部门公司也应做到这样	2000 年 12 月
1.22	展示 PKI-Aware 应用程序的互操作性，比如电子邮件，通过已出版的《证书发行及管理组件的安全要求》征求公众对 PKI-Aware 应用程序互操作性的意见	2000 年 12 月
1.23	不晚于 2001 年，联邦各机构应当在法律要求的范围内向 OMB 和 NIST 报告它们对相关的安全操作建议和联邦信息处理中心（FIPS）采纳的程度	2001 年 1 月
1.24	CIPIS 将整合并协调国防部门级的修正计划，评审国防部门的缓和计划和业务计划的制定，评审 DI 部门重建计划，起草综合的 DI 部门重建计划，起草各种有效性评测方案	2001 年 3 月
1.25	使用经签名的电子邮件，所有的电子邮件都将被签名，在整个国防部的范围内，鼓励对邮件进行加密	2001 年 10 月
1.26	首次检验 PKI 组件对《证书发行及管理组件的安全要求》的满足程度	2001 年 12 月
1.27	国防部将向其所有 PKI 用户发行最安全的证书/令牌	2002 年 1 月
1.28	各防卫部门将完成与基础设施依赖性和国家国防基础设施关键性评估有关的风险管理原则的制定和应用。完成这一任务将依靠：制定并实施一致的风险管理框架，确定风险和不确定性的来源，确定因果关系，认识可能性和结果的影响范围，评估极端事件，考虑极端事件带来的风险，确定和分析各个可能的选项	2002 年 12 月
1.29	修正计划应已经消除了联邦机构和主要公司的关键信息系统绝大部分已知脆弱性。脆弱性评估和修正还要继续下去	2003 年 5 月

范围注解

保护计算机和物理关键基础设施

保护国家的关键基础设施一直以来是政府关注的主题。水坝、桥梁、隧道、电厂和其他重要的物理建筑物已经被特别保护了 50 多年了。1995 年，PDD39 指示总检察官负责开展了一次政府范围内的检查工作，以确定政府范围内的基础设施是否得到了足够的保护。

总检察官的检查突出显示了我们缺少对计算机基础设施——关键信息系统和网络——保护工作的重视。这次检查结果直接决定了关键基础设施保护总统委员会（PCCIP）的诞生。PCCIP 发现了关键基础设施保护工作中的很多脆弱性，却找不到任何系统和程序去解决这些脆弱性。

因此总统在 PDD63 中阐述了他的意图：美国将消除那些被“针对我们的关键基础设施——特别是计算机系统的物理和计算机攻击”所利用的弱点。

为了重新研究非计算机系统的物理弱点，FBI、DoD 和其他机构将评审 1995 年的工作，在必要的地方对这些工作进行更新，调整 FBI 的关键资产初步活动（KAI）和国防部（DoD）的关键基础设施保护项目。

一个新的关键物理基础设施保护计划正在开发之中，该计划将包含很多活动项目来确保对这些基础设施的保护。DoD、FBI 正同 CIAO 合作，一起领导这个计划的开发。一旦完成，信息系统保护国家计划和这个新的关键物理基础设施保护计划就连接起来了，使我们可以采用横向的视点对其进行观察。计算机保护计划的第 2 版及以后的更高版本会反映出这种横向视点。这两项计划未来可能会被合并。

计划 2：检测攻击和非法入侵。

“今天，我们甚至不知道我们是什么时候被攻击的。”

计划 2 为我们的敏感的计算机系统安装了多层保护，包括先进的防火墙、入侵检测监控器、异常行为识别器、企业级管理系统和恶意代码扫描设备。为了保护关键的联邦系统，计算机安全操作中心[先是在国防部，然后是与其他联邦机构相协调的联邦入侵检测网络（FID Net）]将收到来自这些检测设备的警告，也可以从计算机应急响应小组（Computer Emergency Response Teams，CERT）或其他途径获得攻击警告，用来分析并协助各站点抵御攻击。

我们确认和修正脆弱性的工作能够延缓但不能阻止对信息系统的恶意入侵。通用软件仍将继续具有脆弱性，不同软件和硬件组合中的相互作用也会产生安全上的漏洞。对系统有访问权的心怀不满的雇员会经常制造严重的破坏，他们的反常行为却可能长久地被人忽视，直到亡羊补牢为时已晚。

考虑到系统和软件的脆弱性，以及可能受侵害的目标系统的数量和非法入侵的频率，检测和监控系统的开发和使用势在必行。这些入侵检测系统已经在行政部门和国会中得到了应用。增强系统安全性的关键性的下一步就是在整个联邦部门和机构中安装入侵检测监控器，并且要有一个能够对系统异常进行中央分析的功能模块。

社会生活中有很多报警器互连的成功例子。比如，住宅报警系统——当私人住宅遭到入侵时，当地警局的报警器如果不会自动报警，私人防盗系统就会失去效果。

- 安装入侵检测监控器和防卫检测系统。

检测网络中非法入侵行为的第一个必要步骤就是安装和使用高度自动化的应用程序，包

括如下四类防卫检测系统。

第一，在防火墙两边安装的入侵检测监控器，该监控器要定期更新。

第二，授权用户访问和活动的规则以及一个检测程序，以确定一个明显的授权用户所出现的异常行为。

第三，企业级的管理程序，可以确定网络上有哪些系统，知道它们正在做的工作，还可以加强访问和活动规则并进行安全升级。

第四，用来分析操作系统代码和其他软件的技术，以确认是否存在恶意代码（比如逻辑炸弹等）以及其他类似后门的危险代码（不管其初衷是恶意的还是善意的）。

本计划号召在联邦关键信息系统网络中的以上四类防卫检测系统中的合适地方安装同类产品最优程序。在政府内部，这些安装可能通过政府指令来完成。政府还可以通过信息共享及分析中心（ISAC）对这类系统做出评价（见计划 4）。

- 入侵检测监控器的网络系统。

为了保护民用机构（非国防部）中的关键联邦系统，国家计划还要求将保护单个政府系统的防卫检测系统和总务管理局的联邦计算机事件响应能力中心（FedCIRC）的中央分析单元联系起来。后者可以对多种网络的系统异常进行实时分析。如果联邦机构或者 FedCIRC 认为已经掌握了非法行为的足够证据，它们将通知 NIPC，以进行下一步的行动。只要任意一个站点遭到攻击，有关攻击的警告词汇立即就会引起其他站点的注意。

在目前的技术水准下，该系统——联邦入侵检测网络（FIDNet）——以及其他的网络监控系统需要自动感应和人工管理相结合。自动系统要求对政府网络内部关键节点上的系统异常性数据进行有效收集。现在，系统异常分析在很大程度上依赖于各机构内的人工处理，一般由 GSA FedCIRC 内受过专门训练的分析员来完成。随着研发的深化，越来越多的分析将使用人工智能工具自动完成。此外，我们还需要有面对入侵时能迅速更新系统防卫的自动化工具。

有三个系统共同支撑着美国政府的关键系统保护功能，FIDNet 将成为其中之一。

国防部计算机网络防护联合特别任务中心（JTF-CND）已经建立起来，正在对国防网络进行监视，并可以在遭到入侵/攻击后对功能恢复行动进行协调。

国家安全事件响应中心（NSIRC）为 JTF-CND、CIDNet 和 NIPC 提供专家帮助，协助它们隔离、通知以及解决危害国家安全系统的攻击和非法入侵。NSIRC 将和 JTF-CND、CIDNet、NIPC 一起协调对这些直接危害国家安全系统的攻击和入侵所做的事件报告和对脆弱性的评估。

联邦入侵检测网络（FIDNet）是为了保护联邦民用部门的关键信息网络而创立的，它以国防部系统为模型，在 GSA 执行和操作。在法律的范围内，当非法行为的某种迹象需要得到 NIPC 的分析和警告部门的分析支持或者报警通知时，FedCIRC 将同 NIPC 进行协调。同样，当需要 NIPC 的计算机调查和执行部门的犯罪调查或国家安全调查时，FedCIRC 也将寻求与 NIPC 的协作。

司法部的初步审查认为，FIDNet 的理念同电子通信隐私法案是一致的。综合的法律评审——由各机构的代表实施——正在进行，以确保 FIDNet 在建设中同政府的隐私和公民自由政策、法规及宪法的规定保持一致。计划 2 时间表见表 3.2。

表 3.2　计划 2 的时间表

阶段	活动	目标时间
2.1	在空军、海军、陆军以及国防部建立连接入侵检测系统的分析机响应中心。建立国家安全事件响应中心（NSIRC）	已完成（1998 年）
2.2	在关键性国防部系统中安装第一批 500 套入侵检测监控器	已完成（1998 年 12 月）
2.3	建立国防部范围内的集线器用于入侵检测系统——计算机网络防护联合特别任务中心（JTF-CND）	已完成（1999 年春）
2.4	发布部门计算机安全计划，在安全和应急处理办公室管理下重组能源部 CIO 办公室	已完成（1999 年 9 月）
2.5	对联邦系统中的恶意代码进行初步分析	2000 年
2.6	建立一个用于联邦民用机构的入侵检测网络（FIDNet）试点，到 2000 年 10 月要有 22 个关键性联邦网络连入	2000 年
2.7	对访问/活动监控进行升级，在联邦系统的合适地方建立企业级管理系统	2000 年
2.8	完成具有自动化处理和可适应性功能的大型入侵检测网络上伸缩性问题的处理以及其他事项的研发	2000 年 10 月
2.9	开发并定期升级检测系统的标准	2000 年 10 月
2.10	在联邦政府需要的地方对防火墙和入侵检测监控器进行升级	2001 年 1 月

计划 3：开发稳健的情报和执法功能，与现行法律保持一致。

“人民组成政府是为了保卫人民，防御国外敌人和国内犯罪。”

计划 3 将帮助和加强美国执法及情报机构并转换它们的角色，使它们能够处理计算机网络所面临的新型威胁和新型犯罪。

过去，国外对我们国内基础设施的威胁主要来自轰炸机、洲际导弹和潜艇。这些系统可以被情报机构定位和计算出来。但现在，我们的基础设施遭到的是基于计算机的攻击威胁，其危害度和来源很难发现并估计。

依据第 12333 号行政令、总检察官指导方针和中央情报局长的指示协议，美国情报机构最应该做的是收集国外信息战能力和意图的信息，这在所有的优先级中排在第一。

情报机构要收集潜在的国外敌人的计划和攻击能力的信息，这是非常重要的。但是，收集计算机攻击威胁信息比收集传统军事威胁情报面临着更多困难和挑战。情报共同体正致力于开发新的解决方案，以应对这种艰难的挑战。

对计算机网络的攻击，无论是物理的还是计算机的，一般来说都违背了联邦或者各州的法律。要证明攻击已经发生、找到攻击者并证明其罪行需要新的技术，使执法、情报分析和国家安全响应能实现无缝结合。FBI 的国家基础设施保护中心（NIPC）是一个跨机构的保护中心，它使用来自各种资源的信息——包括开放资源、民营部门、执法和美国情报共同体——来提供攻击的早期警报，并通过收集在确定攻击方时必要的信息，对攻击做出部分响应。而且 NIPC 还有执法和国外反谍报的使命，并在该领域内的负责机关的领导和协调下进行操作。中心有来自国防部、情报部门、NSA 和其他联邦机构的代表。中心的角色是，作为牵头部门，开发和改善一系列相关功能，用于判断入侵开始时间、分析攻击范围和攻击源以及寻找攻击者。

可能攻击的警告、某些合适的攻击事件和脆弱数据，都将被民营部门、州及地方政府共享。这些信息对于 TIGA 的防卫能力来说非常重要（见计划 4）。

通过其他项目的努力，美国执法机构严格化的国内执法机制和工具正在改进。司法部的计算机犯罪和知识版权处以及美国检察官办公室，都通过计算机电信协调中心项目增加了受过技术训练的公诉官的数量，从而加强了我们对计算机网络犯罪的起诉能力。

我们还与其他国家的可信执法伙伴进行了合作，以建立国际合作系统，开发通用的方法对非法入侵和计算机系统攻击进行定罪。

我们决心做到，对于任何滥用计算机技术的人，不管他们是为了获取非法利益还是怀有其他邪恶目的，也不管他们这样做是为了国家、恐怖主义分子还是犯罪组织，我们一定要找到他们并将其绳之以法。我们不会因为他们的罪行源于或超越了一个或多个其他国家的审判权限而放过他们。同时，我们还要开发与现有规则和政策相一致的很多其他政策和项目——这些政策和项目将主要关注国内执法部门和国家安全机构在各自的国内外行动中的法定角色。计划 3 时间表见表 3.3。

表 3.3　计划 3 时间表

阶段	活动	目标时间
3.1	提高联邦执法部门和情报机构对于收集、追踪以及分析计算机威胁和关键信息系统脆弱性的注意力	已完成（1999 年）
3.2	情报共同体、国防部以及联邦执法部门发起一系列工作组来开发新的适于对付计算机威胁的信息收集技术以及分析技术	2000 年

计划 4：实时共享攻击警报和信息。

“攻击一点应视为攻击全体。”

1998 年 2 月首次发现针对空军计算机的“Solar Sunrise”攻击时，我们还没有足够的措施和方法了解这些攻击是否也针对其他的国防部系统以及关键联邦网络或者关键民营部门系统。今天，已经有了全国范围内的系统来对攻击进行实时的信息传递。

首先是经过改良的联邦信息共享。在不久以后的一段时间内，我们需要用我们已有的数据来完成更好的工作。联邦系统管理员有大量的关于异常和可能入侵的广泛数据，他们应该把这些数据发给 FedCIRC，包括 FIDNet 系统的增强功能模块。非法行为和入侵的迹象将被直接提供给 NIPC 分析。FedCIRC 还是重要的事件数据接收者和提供者。得到了所有这些资源的信息之后，NIPC 和 FedCIRC 将把这些报告同它们手头的其他信息结合起来，判断出入侵的模式或者那些貌似随机的事件之间的联系。

在国防部内部，国家军事指挥中心和 JTF-CND 将接收、巩固和评估国防部各部门报告，发现国防部内的入侵迹象并将它们报告给 NIPC，发布国防部警告，接收、评估和发布国家警告。

对于私人业主和州及当地政府，这个计划鼓励信息共享和分析中心（ISAC）的建设。它将在公司和各州及当地政府之间共享信息，并接收政府的警告信息。有关 ISAC 和信息共享的白宫会议曾召开过，被 PDD63 指派为部门联系地的几个联邦部门也曾主持过几个会议（包括财政部前部长 Robert Rubin 和能源部部长 Bill Richardson 主持召开的会议），作为这一

系列会议的结果，一些工业组织，包括通信和财政服务组织，已经决定建立 ISAC。其他工业组织正在评估这个提议。

NIPC 将向各 ISAC 提供威胁、脆弱性和相关事件的信息。

ISAC 以资源的方式——对于那些愿意这样做的公司来说，绝对不是强制性的——把入侵和其他攻击信息通知给联邦各机构。发送信息之前 ISAC 可以预先对信息过滤（比如，删掉信息中公司的名字）。然而，我们提倡各公司直接向当地的 FBI 区域榜公示报告计算机攻击事件。

银行和金融部门 ISAC

1999 年 10 月 1 日，美国财政部部长宣布开放银行和金融服务信息安全设施——金融服务信息共享和分析中心（FS/ISAC）。

这个中心是一个民营政府与民间机构的合作项目，用来促进对金融服务业计算机攻击信息的共享。它为这些攻击信息提供了一个快速发布的匿名场所，提高了金融服务界对其技术基础设施受到的攻击进行防范、检测和响应的能力。

FS/ISAC 的成员资格向所有已获得或认可的财政服务协会的成员开放。目前，已有代表私人和公共利益的 12 个组织签署了信函，表明了它们对加入这个中心的兴趣。FS/ISAC 由私人承包商管理，并由各会员公司全额资助。

为信息共享排除障碍。很多公司可能希望和政府专家讨论可能的系统脆弱性，但又存在顾虑，因为根据《信息自由法令（FOIA）》，如果它们把信息透露给政府，那么同时可能会被要求把信息向公众透露。关于政府脆弱性的敏感信息已经得到了现有法律的保护，不必因 FOIA 而向外泄露。为了推进这个国家计划，关键基础设施保护办公室（CIAO）和司法部共同召开了关于信息自由的白宫会议，与会的还有公共和民营部门的专家。与会者讨论了 FOIA 对信息共享可能造成的妨碍。通过民营部门的加入，一个跨机构工作组已经成立，其任务是推荐可能的全面解决方案。民营部门所关心的其他一些法律关注问题，包括反垄断和责任问题等，也将得到类似的处理。

垄断 FIDNet 和 JTF-CND。在隐私和执法限制条例的许可范围内，FIDNet 和 JTF-CND 事件检测系统将共享事件数据。

国家安全事件响应中心（NSIRC）将从 FedCIRC 和 JTF-CND 获得数据，进行细致的事件分析和脆弱性评估。NSIRC 脆弱性评估将用于开发硬件和软件计算机网络防卫系统。

计划 4 时间表见表 3.4。

表 3.4　计划 4 时间表

阶段	活动	目标时间
4.1	司法部和关键基础设施保障办公室（CIAO）在白宫会议中心召开一次关于《信息自由法令》和保护关键系统脆弱性信息的会议	已完成（1999 年 7 月）
4.2	在国家基础设施保护中心（NIPC）建立 24 小时全天候计算机攻击通知功能模块	已完成（1999 年）
4.3	开发用于同民营部门的各个信息共享和分析中心（ISAC）进行安全信息共享的机制	2000 年
4.4	CIAO 和总务局（GSA）将为各联邦政府的 CIRC/CERT 发起一次白宫会议，推动这些公共运行系统的协调和发展	2000 年

续表

阶段	活动	目标时间
4.5	提交法律方面的修订议案（如果需要），以帮助 ISAC 的建设	2000 年
4.6	和民营部门集团合作，在几个重要产业部门建立 ISAC	2000 年及以后
4.7	在州级别上同多个州级权力机关一起建立“测试床（test-bed）”或计算机安全信息共享项目样板	2000 年
4.8	建立其他的信息共享和分析中心	2000 年

新墨西哥州关键基础设施保护委员会

保护关键计算机系统及物理基础设施的全州范围内公私合作的样板

新墨西哥州关键基础设施保护委员会（NMCIAC）是一个私人与公共部门的合作机构，它的建立最初是为了商业团体、工业、教育机构、联邦调查局（FBI）、新墨西哥州政府和其他联邦、州及地方机构之间的信息交换，以确保对新墨西哥州关键基础设施的保护。NMCIAC 致力于研究威胁、脆弱性和对策，还针对基础设施攻击、非法系统入侵以及可能影响 NMCIAC 成员组织和/或普通民众的那些因素所采取的各种响应进行研究。物理的以及计算机的保护都是通过对关键系统的威胁信息进行参照和传播来完成的。在计算机和物理保护方面，NMCIAC 同 FBI 的 InfraGard/NIPC 活动结成了联盟。

NMCIAC 是美国第一个完全由自愿者组织的全州范围内的组织，为其他 49 个州内类似组织的发展提供了原型。在诞生后相对较短的时间内，它就招募了代表私人和公共部门的 36 个组织。NMCIAC 使用工作组的形式完成其主张的目标。这些工作组依据不同的关键基础设施领域来定义：信息和通信，公用事业（天然气、石油、电力和水供应），银行和金融，运输，紧急事务管理，紧急情况和政府服务，信息共享和分析中心，管理和操作。

NMCIAC 定义了六个主要任务：

- 建立并管理以各州为基础的信息共享和分析中心（ISAC）；
- 创建并操作一个先进的安全通信系统；
- 确定并评估用来减弱威胁、威胁响应和事后恢复的技术；
- 发起并完成一个训练、推广、技术转让和技术协助项目；
- 开发并共享一个州级的关键基础设施保护模型；
- 管理和操作 NMCIAC。

为了迎接挑战并鼓励参加，NMCIAC 给它的成员提供了很多利益，包括：一个入侵报警网络；一个只为成员开放的信息提供网站；用来游说工业界做出必要改变和改善的工具；训练讨论会，帮助各成员完成其职责；各成员自己开发的项目，可以在各自的组织内分别执行。

对于那些有兴趣通过合作来保护其关键信息系统的其他工业部门和州及地方政府实体来说，NMCIAC 的成功是一个指路的明灯。从 NMCIAC 中获得的经验能使我们社会的各个部门在关键基础设施的保障中受益。事实上，NMCIAC 官员正在同弗吉尼亚州官员合作，以期在该州开发一个类似项目。

信息共享和分析中心能为工业界做什么

国家计划号召工业协会或集团建立工业范围内的计算机安全中心，称为信息共享和分析中心，这些中心将做到：

- 在各公司间就脆弱性、企图的攻击和非法入侵的性质做到信息共享，这些信息可以被中心“过滤”以防止人们知道是哪个特定公司遇到了计算机事件；
- 协调产业界的特殊研发需要；
- 检查整个产业范围内的脆弱性和依赖性；
- 开发雇员教育和意识培养项目，共享雇员培训项目。

政府怎样帮助信息共享和分析中心

国家号召政府通过如下措施对信息共享和分析中心进行协助：

- 提供重要攻击的实时数据，对网络面临的威胁进行战略性评估，提供攻击技术的信息，提供脆弱性信息；
- 协调联邦和工业界在信息系统安全方面的研发，帮助满足市场驱动力的需求；
- 为教育和意识培养计划提供资源及其他支持；
- 为了培养工业范围内的 ISAC，对有关信息自由、责任和反垄断等问题的可适用法律做出必要的改变。

计划 5：建立响应、重建和恢复能力。

“……对破坏进行隔离并使其最小化……迅速恢复必要的能力。”

计划 5 是在攻击进行的时候对其限制；使团体和机构保持其职能的连续性；制定恢复计划，以对付信息攻击。

就其规模来说，信息战攻击可能不会限于一个个孤立的事件。它们可能是在一个工业系统或机构内发动，也有可能出现于一个完整的经济部门、国家的一个地区或者国家本身。通过使用 JTF-CND、FIDNet 和工业集团的 ISAC 所提供的攻击数据，NIPC 将和各联邦机构及民营部门合作，以确定正在进行的攻击的范围。

一旦一个大范围内的攻击得到确定，中心将与执法部门和其他机构协同工作，对攻击做出响应，包括向系统管理员建议执行一系列计划措施：

- 阻断可疑用户进入网络的通路；
- 实施特殊“防卫状态”安全警戒；
- 针对攻击所采用的技术，应用新的安全软件“补丁”；
- 隔离网络的某些组成部分；
- 中止某些网络运作；
- 启用紧急事件下的接管系统。

与此同时，执法部门和其他相关机构将对攻击源进行定位并采取合适的措施将其中断。我们鼓励民营部门和执法部门之间关于攻击响应行动多做协商，以免民营部门的行动对入侵调查造成不必要的阻碍，防止抹掉入侵者的属性特征甚至延误对入侵者的起诉。

政府的目标以及我们对工业界的建议是，每一个关键性信息系统都要准备响应计划，这些计划中要包括如下响应行动所做的准备：迅速启用其他的防御措施（比如，更为严格的防

火墙要求）；在某些预定情况下关闭部门网络（通过企业级的管理系统）；把最小化基本操作交由“干净”系统运行；迅速重建受感染的系统。

在很多情况下，企业和机构的恢复计划只集中或主要集中于物理破坏：洪灾、暴风雪或爆炸等使总部瘫痪的事件。仍继续把各种指令发往各公司或机构的信息系统网络中。现在这些计划中通常包括“备份”计算机数据库，用于总部系统不存在或无效的情况下。

如今，恢复计划还必须能够应付所有或部分信息网络本身被破坏的情况。这时，一定要有替代的方法用来传递最小量的重要信息。专家组要立刻赶到以协助重建工作，包括分析导致网络瘫痪的软件错误以及设计代用方案等，还要负责网络重启。

在这个世纪之交，我们有可能遇到同“千年虫”有关的崩溃事件，可以创建“千年虫”信息协调中心来协调事件信息流。这个中心由政府和工业界的专家联合组成，并和国家信息中心（NIC）的系统合作。后者的职责是收集各部门的状态信息。

在 PDD67 中，总统指示每个联邦部门和机构在 1999 年年底以前提交保证运作连续性的计划。这些计划要含有在 PDD63 中所述的任何紧急情况发生时保护操作连续性的措施。

联邦部门联络官将同各自对应的产业界合作，确保企业的恢复计划中也同时提及了信息攻击重建。商业部跨机构的基础设施保障办公室（CIAO）将发起一次有保险业和审计业参加的白宫会议，并同它们开展持续的对话，以促进对风险管理、操作建议以及衡量标准的理解。

计划 5 时间表见表 3.5。

表 3.5　计划 5 时间表

阶段	活动	目标时间
5.1	各部和机构将修改其操作连续性计划，考虑进行意外事件以及 PDD63 中谈到的紧急事态	已完成 （1999 年 12 月）
5.2	关键基础设施保障办公室（CIAO）将发起一次有审计和保险业的代表以及部门协调中心参加的白宫会议，会议集中关注商业重构和审计界在信息时代的新角色	2000 年
5.3	JTF-CND 以及其他政府机构将为政府信息攻击报警网络开发协议和建议	2000 年
5.4	联邦应急管理局（FEMA）将进行紧急通信系统的现代化改造	IOC：2000 年 FOC：2000 年

计划 6：为支持计划 1～5，加强研究和开发。

“信息技术正以互联网年的速度发展着，　一个日历年的时间相当于四个互联网年。”

计划 6 系统地确立了实现这个计划所必需的研究要求和优先级顺序，确保了研究资金来源；而且，该计划中还建立了一个系统，用来保证我们的信息安全技术始终紧跟整个信息系统中的威胁的变化。

只依赖现有的技术，计划 1～5 所要求的很多任务是无法有效开展的，甚至有些情况下全然不能执行。跨机构的关键基础设施协调组（CICG）已经建立了一套步骤来确定计划的技术要求。由科技政策办公室（OSTP）领导，研究和发展子工作组将与各机构和民营部门合作，就信息安全研发的要求和优先级取得一致意见；在联邦各部和机构中进行协调，保证部门研究预算的要求得到满足，防止部门工作的浪费和重复；与民营部门和学术研究院交流，防止联邦资助的研发与民营部门及学术界以前、正在进行和将要进行的计划重复；确定在信

息安全技术中，市场还没有投入足够或充分研究工作的领域。该过程始于 1998 年，在 2000 年的行政预算中，这些基础设施保护研究将花费 5 亿美元。过程所确定的要优先研发的项目包括：

- 支持大规模入侵检测监控网络的技术；
- 能够确定操作系统代码中恶意代码（后门）的人工智能及其他方法；
- 在攻击或灾难中能够控制、阻止和驱逐入侵者并减弱破坏程度或恢复信息处理服务的方法；
- 可以增强网络可靠性、系统生存力、关键基础设施部件和系统乃至关键基础设施本身的稳健性的技术；
- 对基础设施响应进行建模的技术，确定互依赖性及它们的含义，定位主要的脆弱节点、组件或系统。

CICG 的 R&D 子工作组在 1999—2000 年发起的一系列会议

CIGG 的 R&D（研发）子工作组正在发起很多讨论组来研究那些受关注的、横向的研发主题：

- 入侵、恶意代码和异常行为检测（1999 年 2 月 22～23 日）；
- 关键信息系统基础设施间的相互依赖性（1999 年 8 月 11～12 日）；
- 恶意代码（时间待定）；
- 内部人士威胁（时间待定）；
- 入侵检测（时间待定）；
- 重建/恢复（时间待定）。

计划 6 时间表见表 3.6。

表 3.6　计划 6 时间表

阶段	活动	目标时间
6.1	协调联邦政府关键基础设施保护研发工作，为 2000 年及后续财政年度的预算做准备。确定国家计划执行中需要的研发项目，制定多年度的资金战略，并把第一年的资金要求纳入 2001 年度部级预算需求之中	已完成 （1998 年 6 月）
6.2	通过咨询民营部门和学术界，科技政策办公室（OSTP）将每年更新联邦政府关键基础设施保护研发项目中的优先级	1999 年 9 月 由此继续
6.3	召开有产业界、学术界代表和政府专家参加的会议，讨论研发项目的优先权，建立公私机制来协调联邦和民营部门对关键基础设施保护的研发，协调计划 7 中人力和训练方面的工作与资源，建立并支持培训方面研究的发展，使本科生和研究生具有熟练的技术	1999 年 12 月 由此继续
6.4	确定国家计划所需的主要研究项目的完成日期	2000 年 1 月
6.5	对创建中央 R&D 联邦基金进行评估，以对横向项目进行支持，确保 2002 年及后续年度预算中政府与民间研究的协调	2001 年 3 月
6.6	建立信息基础设施保护学会（I^3P），对各类研究项目进行资助	2001 年

计划 7：培训和雇用足够数量的信息安全专家。

“我们所缺少的恰恰是经过专业培训的人。”

计划 7 概览了联邦和全国范围内信息安全专家的数目和所需的技术，采取了措施来训练现有的联邦 IT 雇员，并征募和教育其他人员来弥补这种人才的缺口。

有证据表明，在全国范围内，我们面临着熟练的 IT 人员越来越供不应求的危险。尤其是信息系统安全人员这一子集更加缺乏。在联邦政府内部，熟练的信息系统安全人员的缺乏也发展成了一种危机。雇员的匮乏反映了大学研究生和本科生的信息安全课程实在太少。为了解决这些问题，我们将调节并依靠国防部、国家安全局、CIO 委员会和各种联邦机构的工作。

联邦计算机服务（FCS）的训练和教育活动引入了五个项目来帮助解决联邦 IT 安全的人员缺少问题。

完成认识管理办公厅 IT 职位研究。该研究将有助于确定联邦政府 IT 职位的数量。

发展信息技术卓越中心（CITE）。这些中心将培训和认证现有的联邦 IT 人员，帮助他们在其职业生涯中维持技术水平。这些中心还将利用国防部和其他联邦机构在这个问题上的重要项目成果。

创立服务奖学金（SFS）项目，从而招募和教育下一代联邦 IT 雇员和安全管理员。这个计划将每年资助 300 个学生，帮助他们完成在信息安全领域的本科或研究生学业。作为偿还，学生在毕业后将在联邦 IT 岗位上服务一段固定的时间。计划还将包括一个很有意思的暑期工作和实习计划。SFS 项目的一个主要部分是确定参与项目的大学，对这些大学里的信息安全职员和实验室发展提供帮助。

发展高中招募和培训活动。这一项目将确定有潜力的高中生参加暑期工作和实习，使他们熟悉联邦 IT 工作标准，为将来到联邦 IT 岗位就业做准备。该项目还将检查那些旨在加强中学生计算机安全意识培养的可能方案。

开发并使用联邦 NF OSEC 意识培养课程。该项目旨在确保各个联邦岗位都在开展计算机安全意识教育。它将利用几个杰出的联邦机构意识培养项目。

计划 7 时间表见表 3.7。

表 3.7　计划 7 时间表

阶段	活动	目标时间
7.1	启动在大学的推广工作，以推动 SFS（服务奖学金）项目的发展。对 SFS 候选人进行认证，建立专题讨论会以招募可能的候选人。如果需要，则为任何其他的权威项目制定提议	2000 年 1 月
7.2	对联邦范围内信息系统安全培训和教育项目进行完整的培训，确定现有的培训和教育项目，找出差距或冗余	2000 年 3 月
7.3	为大学申请并被选入 SFS 项目制定标准、备案要求和指导方针	2000 年 4 月
7.4	利用国防部和民营部门的模型，开发联邦 IT 安全雇员认证项目，用于系统管理员和各 ISSO（信息系统安全官）；开发培训项目，用于满足这些认证目标的需要	2000 年 5 月
7.5	开发并传播联邦岗位信息安全意识培养课程。各 CITE（信息技术优秀中心）中，其中一个将负责这一项目，预先审查和更新其内容	2000 年 5 月
7.6	制定指定 CITE 时的标准	2000 年 6 月
7.7	设计和执行中小学推广计划，包括各种会议、暑假工作和实习	2000 年 7 月

续表

阶段	活动	目标时间
7.8	确定参与第一年 SFS 项目的一批大学	2000 年夏
7.9	在联邦政府内完成 OPM（人事管理办公厅）领导的对信息系统安全职位要求的研究。这将为联邦 IT 岗位的人员招募、选择、工资偿付和能力发展提供可靠的数据	2000 年夏
7.10	为未来的 SFS 教职员开展一个实验性的信息系统培训项目。这将成为我们的教职员发展项目的前导	2000 年夏
7.11	为 2001 年开始的第一年 SFS 项目招募研究生和本科生，以后每年招 300 个学生	2000 年秋
7.12	确定、指派各 CITE，并为其提供资源。中心将为联邦 IT 雇员开发和提高质量的信息系统安全培训及认证，还将向 SFS 和暑期工作项目中的中学生提供技术认证和培训项目	2000 年 10 月
7.13	第一批 SFS 项目学生开始学习	2001 年 1 月
7.14	SFS 计划的第一批研究生进入联邦 IT 工作岗位	2002 年 5 月

计划 8：推广，使美国人民知晓提高计算机安全的必要性。

“知前行后。”

计划 8 向公众解释现在就采取行动的必要性，在灾难性的事件到来之前，提高我们抵御处心积虑的计算机攻击的能力。

保卫美国的计算机空间需要所有美国人——商业领导、教育和其他民营机构、政府（联邦、州和地方）以及普通公众——都行动起来。作为国家计划所阐述的很多行动的基础，我们要对信息系统所面临的新威胁以及行动的必要性具有一定的理解和认识。

到目前为止，还没有“电子珍珠港事件”来唤起公众对行动必要性的认识，也没有太多的美国人认识到我们的经济和国家安全对计算机和信息系统的依赖程度——这些系统的功能通常被日常生活屏蔽掉了。

结果，我们不得不做很多意识培养方面的广泛工作。在初始阶段，至少有三项工作要做。

- 通过“网络公民项目（Cyber Citizens Program）”，对美国儿童进行计算机道德和合理使用互联网及其他通信工具的教育。
- 通过关键基础设施安全合作关系（Partnership for Critical Infrastructure Security）项目，打造美国企业领导和信息技术领导的合作关系。在这个项目中，我们都认识到了在民营部门和政府中采取特别措施以提高我国计算机安全的必要性，并在全国范围内公认的项目中实现合作。
- 保证联邦雇员本身能够意识到信息系统安全的必要性。

过一段时间，还将加入第四项工作：以上述工作为基础，把我们的意识培养活动扩展到其他私人组织和普通公众中去。

这些行动构成了我们保卫美国信息基础设施的基础。

计划 8 时间表见表 3.8。

表 3.8　计划 8 时间表

阶段	活动	目标时间
8.1	通过创建计算机公民项目，对美国儿童施以使用计算机系统时适宜行为和道德方面的教育	已完成（1999 年 5 月）

续表

阶段	活动	目标时间
8.2	通过创建公私关键基础设施安全合作关系项目，提高各公司及政府对关键信息系统和计算机网络所受威胁的认识	2000 年 2 月
8.3	向所有可以接触敏感信息系统的联邦政府人员提供计算机安全意识强制性通告。这种强制性通告在他们接触业务时就要提供，并且以后至少每两年提供一次	2000 年 3 月

计划 9：采用立法和拨款手段支持计划 1～8。

“正如政府必须和民营产业形成合作关系一样，行政部门和国会必须紧密合作，共同保卫我们国家的关键基础设施。”

计划 9 为支持其他计划提出的活动提供了法律框架。该计划要求联邦政府内部——包括国会——同民营产业之间紧密合作。

总统已经提出了行动建议，并指示，联邦各部和机构要努力保证自身关键系统的安全，还要同民营部门建立合作关系来保护我国的基础设施。很多类似活动得到了国会的支持，包括在 2000 年预算拨款 17.37 亿美元。

国会议员和各委员会的行动表明，他们也意识到了我们国家关键计算机系统所面临的潜在攻击威胁，而且他们还预先采取了很多保护性措施。我们正在评审现有的法律以及先前引入的立法提议，并正在为提高关键基础设施安全性制定很多新的提议。

正如其他计划中所述，我们需要新的法律以建立产业和政府合作的基石。为了推动民营部门信息共享和分析中心（ISAC）的建设并促进民营部门和政府间的信息共享，在设计同民营部门共享信息的事务时，我们必须有能力保护敏感信息并缓解潜在的责任和反垄断法问题。

为了保证这份国家计划中某些行动的有效开展，我们正在调研建立新的法律机构的必要性。我们时刻考虑着保护公民自由和隐私的绝对需要，因此将制定出法律框架来提高保护关键系统的短期乃至全面的运作能力。

我们需要国会支持总统为计划 1～8 所划拨的预算资金。国家计划中各个时间表内的任务的成功实现也依赖于资金提供的级别。

我们期待着继续和国会进行建设性的对话，讨论保护关键系统的最佳方法和机制，并敦促其积极参与这个国家计划未来版本的制定。

计划 10：在计划的各步骤和各部分中，要全面保护美国公民的自由权、隐私权和私有数据。

“……人民的人身权、房屋产权、著作权和财产权应该得到保障。”

计划 10 与其他计划融为一体，它确保我们在保护关键计算机系统时的所作所为都符合宪法和其他法律的规定。

保护我们的关键基础设施是很重要的，但保护我们的公民的自由同样重要。国家计划中所有的提议与现有法律和隐私期望完全一致。这份国家计划要求每年召开一次关于计算机安全、公民自由和公民权利的政府与民间的讨论会，以保证国家计划的执行者始终关注公民的自由，并且其计算机安全提议要得到政府内外的民权专家和感兴趣者的讨论。

国家基础设施保障委员会（NIAC）由来自联邦政府之外的参与者组成，它将每年对计

划执行中有关公民自由、隐私权、私有数据保护的情况进行审查。

在设计国家计划时融入了《法律第四次修正案》（*Fourth Amendment Jurisprudence*）规定的隐私保护要求。政府检查公民计算机或电子通信计划的任何举动必须与现行法律如《电子通信隐私法案》相一致。公民同敏感性的政府资产——包括政府 Web 站点打交道时，应该被明确告知对他们行动的监视是不是他们能够访问这些资产的先决条件。国家计划要求建立一个相关系统来保证所有受监视的敏感资产都向访问者提示了必要的清除警告。

美国政府已经开始与民营部门合作，为隐私保护制定强制性规则，以确保互联网用户已被明确告知他们的哪些个人信息被他人收集以及这些信息可能的用途。要给用户选择权，让他们自己决定其个人信息的用途，从而确保其数据的安全，为合理访问信息提供便利条件。还要给他们提供援助机制，当他们的个人信息被非法滥用时能够得到帮助。

计划 10 时间表见表 3.9。

表 3.9　计划 10 时间表

阶段	活动	目标时间
10.1	联邦政府与政府外的组织合作，举行每年一次的政府与民间计算机安全、公民自由和公民权利讨论会	2000 年
10.2	NIAC（国家基础设施保障委员会）和其他相关的权威机关将就公民自由、隐私权和私有数据对国家计划的执行情况进行年度评审。另外还将评审政府和民营部门的其他相关活动以及政府对私有数据的处理，以推动更为广泛的信息共享	2000 年

网络空间国际战略

一、序言

网络空间及网络技术使不同国籍、种族、信仰和观点的人得以交流、协作并取得前所未有的成功。如今，通过互联网连接，美国公司的业务可以延伸至全球任何一个地方，为美国民众创造数不胜数的就业岗位和机会；非洲的农妇可以向拉丁美洲的家庭出售手工艺品，从而实现更广阔的经济发展；欧洲的实验室可以利用亚洲生产的硬件和北美研发的软件进行开创性的研究；澳大利亚和中东地区的学生可以通过视频会议共同学习；各国的民众在信息技术的帮助下，可以使其政府变得更加开放和负责。

当前，当各个国家和民众都在使用无处不在的网络时，我们面临着一个选择。我们可以共同努力实现繁荣与安全，也可以向阻碍发展的狭隘利益和过度的恐惧屈服。网络空间安全本身并不是目的，它应是政府和社会必须自愿承担的责任，以确保创新可以让市场持续繁荣，并改善人们的生活质量。当数字世界面临罪恶和入侵威胁时，我们将高度重视以下原则：言论和结社自由、珍视个人隐私和信息的自由流动。

数字世界将不再是一个没有法律约束的疆域，也不再是少数精英的地盘，而应是一个国家和民众共同坚守责任、正义与和平规范的领域。这是一个极好的自我管理的范例，公民团体、学术界、民营部门以及政府一起共同努力，确保对其进行有效管理。最重要的是，自网络空间诞生以来，其不断地成长、发展，并促进繁荣、安全和开放。这是互联网在国际环境中独树一帜的重要原因，也是其如此重要、需要我们保护的原因。

基于这种理念，我提议制定美国网络空间国际战略。这并不是我的政府第一次就互联网政策和挑战发布报告，但这次是我们提出设想，协调美国与国际伙伴在所有网络空间事务上进行的接触。该战略不仅描述了未来网络空间的设想，而且提出了实现这一设想的日程表。该战略向我们国内外的合作伙伴阐述了我们的政策重点，并说明了我们如何才能维护网络空间的特性，以及如何减少我们面临的风险。

互联网本身无法开启国际合作的新纪元。这一任务是留给我们这些互联网的受益者的。携起手来，我们能够一同建设一个开放、互通、安全和可靠的未来网络空间。这是我们追求的未来，我们也邀请世界各国及其人民加入我们的行列。

巴拉克·奥巴马

二、制定网络空间政策

数字基础设施日益成为支撑繁荣的经济、活跃的研究团体、强大的军队、透明的政府和自由社会的基础。信息技术加强了国际交流，并使国际货物和服务的流动更加便利。社会和贸易的联系已成为我们日常生活中不可或缺的一部分。水电供应、航空管制、金融系统等维系正常生活所必需的基础设施都离不开网络化的信息系统。政府如今通过“电子政务”向民

众提供基本的服务。社会和政治运动也依赖互联网形成新的、影响力更大的组织和行动。网络化的技术在全球无处不在。

对所有国家而言，数字基础设施已经或即将成为重要的国家资产。要在最大程度上实现网络化技术可能带给世界的利益，网络系统必须稳定和安全地运行。要使人们对数据安全传输且免遭破坏有信心。要确保信息自由传输、数据库安全和互联网络自身的完整性对于美国和世界的经济繁荣、安全以及促进普遍权利都具有重要意义。

全世界约 1/3 的人使用互联网，而且无数人在日常生活中都会接触互联网。如今，全球拥有超过 40 亿件无线数字设备。半个世纪前，这个数字几乎为零。我们身处一个史无前例的时刻，我们可以借着网络空间的成功，确保美国公民和国际社会未来的安全。

鉴于网络技术能够继续赋予个人能力、使社会更加富裕，并推动研究、发展、创新等构建现代经济发展的重要因素，网络技术必须保持开放性和互通性，这也是网络技术实现爆炸式发展的重要原因。而这一切需要我们对技术原则和有效管理的支持。与此同时，网络必须确保其保持安全和稳定，必须获得个人、公司和政府的信任，也必须对恶意的破坏具有抵抗能力。

网络空间面临被恶意行为破坏的挑战，全世界都应对此有充分的认识，并相应地提升、加强国家和国际应对策略。在网络空间采取的行动将对我们的现实生活造成相应的影响。因此，我们必须制定法律法规，防止网络空间给我们带来的威胁多过利益。要使一个开放、互通、安全和可靠的未来网络空间永远存在，世界各国就必须意识到其面临的威胁，捍卫其安全，并与那些试图动摇或破坏我们日益网络化的世界的人展开斗争。

美国国际网络空间政策的基础根植于这样一个信念，即对美国和世界而言，网络技术拥有无限潜力。过去 30 多年来，美国已经见证了网络技术给我们的经济和日常生活带来的革命性变革。我们也面临着恶意利用、攻击和入侵等网络挑战。当我们调整应对这些挑战时，我们将树立引领世界的榜样。美国将寻求制定鼓励创新的国际网络政策，以促进经济发展和改善国内外民生。在此项工作中，我们所依据的原则不仅着眼于美国的外交政策，还着眼于互联网技术的未来。

（一）构建成功

美国致力于维护和增强数字网络给我们的社会和经济带来的利益。这些利益包罗万象且影响深远。对个人来说，计算机网络已经提升了生产力，促进了经济繁荣，帮助解决了各类缺陷和不足，融合了因语言或疾病而造成的隔离，并使身处偏远贫瘠地区的家庭和亲友建立联系。对社区来说，它提升了应对突发事件的能力，扩大了信息共享以打击犯罪，曝光了腐败行为，为政治活动提供了便利条件，加强了对被忽视议题的关注。对商业来说，它开拓了市场，培育了价值数十亿美元的产业。对政府来说，它提升了决策透明度，提高了工作效率，增加了便利，并使领导人与其服务的民众之间得以联系和沟通。对国际社会来说，它提供了一个新的全球思想市场，为应对灾难提供了更加便利的解决渠道。信息流通越自由，我们的社会就越牢固。若运用得当，这些技术将全面增强我们的力量，我们将致力于进一步拓展网络技术的应用领域，并改进其在国内外的运作。

（二）认清挑战

美国认识到网络技术的增长给我们的国家安全、经济安全以及国际社会所带来的挑战。

这些挑战包含多种形式，其中包括能够破坏美国本土及海外光缆、服务器和无线网络的自然灾害与事故。技术性挑战也同样存在，如一国采取封锁网页的措施，将导致更大规模的国际网络的中断。勒索、诈骗、身份盗窃都将打击网络用户从事网络商务、社交的信心，甚至危及个人安全。对知识产权的侵犯将威胁到国家竞争和推动竞争的创新精神。这些挑战跨越了国家的边界，网络空间的低成本进入和匿名的特性将使其成为犯罪分子的“安全天堂”。随着传统冲突形式扩展到网络空间，网络安全甚至会在更大的范围内威胁到国际和平与安全。

（三）依据的原则

美国将在坚持我们的核心原则的同时应对这些挑战。我们的政策是既要确保网络空间的有效利用，又要捍卫我们的原则。我们的国际网络空间政策反映了我们对基本自由、个人隐私和信息自由流通的核心承诺。

1. 基本自由

我们对言论和结社自由的承诺是一贯的，但它必须以不危害公共安全和保护民众为前提。在这些公民自由权利中，被国际认可的“基本自由”——如通过媒体不受国界限制地收集、获取和传播信息的能力，已经变得前所未有地重要。作为一个国家，我们并非对抱有恶意企图的网络使用者视而不见，但要辨别这些不属于网络言论自由的例外，我们还需要谨慎行事。举例来说，儿童色情、煽动暴乱和策划恐怖活动在任何社会都是被禁止的，因而在网络上也无容身之所。但美国仍将以遵循我们核心价值观的方式对它们进行打击——采取个别议题个别处理的方式，而不是对网络在社会中的价值进行全民公投。

2. 个人隐私

我们的战略将我们的职责与保护我国公民及我们对其隐私的承诺结合起来。随着民众越来越多地通过互联网参与公共及个人生活，他们对隐私的保护也有更多的期望，即个人应当知晓其个人信息如何被使用，并确信其得到合理的处置。同样，他们也期望受到保护以免受诈骗、偷窃和危及其个人安全的威胁，希望执法部门利用各种手段和措施，根据法律追查和起诉那些恶意利用网络的用户。美国将努力确保两者间的平衡。在授予执法部门必要的调查权的同时，通过适当的司法审查和依据法治原则的监督来保护公民的个人权利。

3. 信息自由流通

对国家而言，没有也不应在确保信息自由流通和网络安全之间做出选择。最有效的网络安全解决方案应当具有活力和灵活性，并将其对网络运作的影响降至最低。这些措施将在确保系统安全的同时，做到不损害创新、不压制言论和结社自由、不妨碍全球的互通性。相反，我们认为其他措施——如国家级的过滤网和防火墙——仅仅是提供了一种虚幻的安全，同时还损害了互联网这一开放、互通、安全和可靠的信息交换媒介。在商业领域也同样如此，网络必须确保成为一种鼓励创新、进取和勤奋精神的平台，而不是某些国家通过蓄意阻断信息的自由流通来获取不公平优势的领域。美国致力于建立一个增强网络安全的国际倡议和标准，在确认我们的全球责任和国家需求的同时，保护自由贸易和更大范围的信息自由流通。

以往这些原则常被认为有悖于有效执法、匿名、儿童保护和基础设施安全。但事实上，可靠的网络安全可以增强对隐私的保护，打击各类非法行为的有效执法可以保护基本自由。

通过尊重法律和捍卫民众利益、稳定国际市场并使全球的恶意网络行为者受到惩罚，法治既支持和维护了我们的国家安全，也促进了我们共同的价值观。

三、网络空间的未来

我们对未来的设想是，可靠的互联网服务遍布全球每个角落，而每个商业机构和家庭都能承受其价格。“无缝连接”的全球网络平台把世界各地的电脑连在一起，使人们得以与同一街区或全球的朋友或同事进行可信的即时交流。交流可以通过各国语言，并在国界之间自由流动。得益于数字翻译技术的发展，数以百万计的人们可以自由地接触到丰富的知识和新的理念，并进行有意义的辩论。最需要的人群能够分享到旨在改良农业或促进公共卫生的新技术，各国专家和发明者们在全球范围内的协作也有助于解决诸多难题。这就是美国追求的网络空间未来的一部分，也是我们一定要努力实现的未来。

根据这一未来设想，个人和商业机构能方便而快捷地获取必要的工具，从而在网络上建立他们各自的天地。人们可以自由获取安全和妥善保管的网络域名与地址，不需要申请许可证，也不会出现随意泄露个人信息的现象。世界各国最优秀的工程师通力合作，开发出信息系统的新标准，从而使网络变得更为快捷、可靠，并能够促进创新，增加网络接入。高技术产业与其顾客一起努力，针对顾客的需求，提供更安全、更可靠和更负责的软件、硬件及服务。

根据这一未来设想，公司和高校可以自由研发新的概念和产品，因为它们知道知识产权和数据是安全的，即使在共享网络中也是如此。每个人都知晓其个人电脑受到的威胁，并能采取简便易行的措施保护他们的电脑系统。民营公司对其网络环境各负其责，因为它们知道，这样做就是保护自己的投资。如果发生网络安全事故，需要政府采取行动，有关官员能及早发现这些威胁，并在第一时间共享有关信息，以阻止恶意软件的传播并最大限度降低大规模混乱的影响。当然，这是在保持信息广泛自由流动的前提下进行的。当出现跨国犯罪时，执法部门可以相互协作，保护并分享证据，最终将罪犯绳之以法。

这一未来设想不仅会推动实现更广泛的繁荣和更可靠的网络，还有助于增强国际安全和更为持久的和平。在这一场景下，国家要成为网络空间中负责任的行动者——要么以不损害他人的方式构建网络，要么阻止犯罪分子把互联网作为安全天堂，进行违法活动。各国都明白保护网络基础设施的必要性，也正在采取措施防止出现混乱和遭到破坏。各国将继续在双边、多边和国际层面进行协作，为世界进入信息时代多作贡献，并就致力于保护互联网及其核心特性达成共识。

美国和越来越多的伙伴国已为这一未来奠定了基础，但远未大功告成，我们也不可能单枪匹马完成这一工作。尽管这一进程可能是缓慢和耗费资源的，但国际社会必须共同努力推动这一长期性的投资。我们为之努力的时候，必须清楚地认识到，对网络空间的这一设想既符合国家利益，也与国际社会的共同目标并行不悖。我们是否取得成功的衡量标准就是，我们是否能够像先前 50 年那样，继续实现今后 50 年信息技术的不断转型和更新，并把风险降至最低。

（一）我们追求的未来

我们追求的网络空间环境将具备以下功能：鼓励创新、赋予个人相应权利、将个人联系

在一起、强化社区的作用、构建更好的政府并提高其可信度、保护基本的自由与个人隐私、增进相互理解、明确行为准则以及提升国家与国际安全。为维系这一环境，国际协作不仅是必要的做法，而且是一项首要的原则。

1. 开放和互通：赋予人们能力的网络空间

数字创新的核心是使网络化的机器拥有新的能力。数字系统的开放性是该系统能实现爆炸性增长、快速发展和持续保持其重要性的根本原因。随着电脑和互联网连接应用于每个国家，网络技术的基本工具得以快速普及，而价格则不断下降。为满足日益增长的网民的需求，硬件和操作系统的生产商必须继续向全球尽可能多的开发商提供相关能力。随着各个公司继续在研发专利软件方面推动创新，我们也欢迎对开源软件进行持续和高强度的研发，从而给予开发商和消费者更多选择，以有效满足其需求。

美国支持互联网实现从终端到终端的互通。有了能够满足各自需求的技术，全世界的人们能够接触到各种知识与理念，并进行相互交流。信息的自由流动取决于互通性——这一原则在突尼斯信息社会世界峰会上得到了 174 个国家的认可。与之相反的是互联网的四分五裂。在这种情况下，世界上大量的人口因为少数国家的政治利益而无法接触到精密的应用技术和丰富的知识。以共识为基础，合作研发信息与通信技术国际标准，是维护开放和互通的关键性工作，这有利于数字经济的增长和推动社会进步。

2. 安全与可靠：长久生存的网络空间

要让当前的网络空间长久生存，我们的网络系统就必须是可信的。广大用户需要相信，他们的数据在传输和存储过程中是安全的，在提供的过程中是可靠的。要执行一项有效的战略，就需要从终端用户到国家间合作多方入手，需要社会各阶层共担责任。

降低网络的脆弱性需要健全的技术标准与解决手段、高效的事故管理、可信赖的硬件和软件以及安全的供应链。在全球范围内减少风险还需要有效的执法能力、全球公认的国家行为规范、建立信任与加强透明的措施、明智的外交，以及相应的威慑能力。最后，事故管理需要与国际社会和民营部门加强协作和共享日益增多的技术信息。它无法由单个国家或某个部门独立完成，需要各个国家及其人民共同承担义务和责任。

互联网的稳定是全球繁荣的基础，而确保互联网稳定的意义绝不仅限于技术层面。经济方面，我们必须推动可持续增长，并对国内外的基础设施进行投资，同时确保网络的可靠性，并明确公司与国家的责任。政治层面，我们必须维持一个尊重技术设施的环境，使分歧不会成为某些人扰乱和破坏网络的借口。社会层面，我们必须使最终用户清醒地认识到，他们有责任以安全和可靠的方式维持和使用网络工具。

3. 通过规则实现稳定

美国将与“志同道合”的国家一起，努力建立一个人们所期望的环境或者相关行为准则，这种环境或准则将符合我们的外交与国防政策并能指导我们的国际伙伴关系。过去 20 年见证了互联网作为一种社会媒体呈现出快速和无法预料的增长，见证了社会日益依赖通过网络信息系统控制对现代生活至关重要的关键基础设施和通信设施，见证了各国政府逐步通过网络空间行使传统国家权力。为消除分歧，我们将努力就“可接受行为”的内涵达成共识，同时与那些同样认为网络系统事关国家和集体利益的人们建立伙伴关系。

（1）规则的作用

在国际关系的其他领域，对“可接受行为”的理解促进了稳定，并在需要采取改正措施时提供国际化行为的基础。坚持上述规则使国家行为具有可预见性，并能防止出现可能导致冲突的误解。

在网络空间推进国家规则并不需要重新构建国际法律习俗，也不需要废弃现有的国际法律规则。指导国家行为的长期国际规则，无论是和平时期或是冲突时期的规则，均可应用于网络空间。然而，网络技术的独特属性，需要我们澄清这些规则应如何应用在网络空间。我们将继续与国际社会一道，努力就如何将上述规则应用于网络空间达成共识；同时，我们也认为，在此过程中，首要的步骤是将人们对于和平、公正的国家行为的期盼反映在网络空间中。

（2）网络空间规范的基础。

有利于推动秩序与和平、有利于提升人类基本尊严并促进经济自由竞争的规则，对于任何国际环境而言，都是十分必要的。这些规则将为所有国家提供一份“基本路线图”，使其清楚应如何行动才不会违反网络空间国际义务，并在任何环境下始终履行自身责任。有利于网络空间规范的既有原则包括以下几项。

- 支持基本自由。各国须明确宣誓并通过其他途径，尊重网络空间以及空间以外的基本自由。
- 尊重财产权。各国应承诺，并通过国内立法确保对知识产权的尊重，包括尊重专利、商业机密、商标权和著作权。
- 尊重隐私。应对个人在使用网络过程中的隐私权加以保护，国家不得随意、非法侵犯个人隐私。
- 预防犯罪。各国必须有能力探知、惩罚网络犯罪行为，以维护法律秩序，防止出现罪犯的“安全天堂”，并及时参与国际犯罪调查合作。
- 自卫权。《联合国宪章》赋予各国正当的自卫权，遭到网络空间攻击后，各国均有权自卫。

由这些传统的国际行为准则所衍生的、更具针对性的网络空间责任，尤其注重维护全球网络的正常运行和提升网络空间安全。这些责任中，有多项根植于互联网技术现状。由于互联网的核心功能有赖于信任体系（如“边界网关协议”），各国应对自身技术决策可能造成的国际影响保持清醒认识，并相互尊重网络权益。同样，在设计新一代网络系统的过程中，我们必须通过支持最合理的技术标准和管理架构来促进共同利益，而不是反其道而行之，仅仅以提升本国声望或加强自身政治掌控能力为出发点。一些正在出现的规范，同样对网络空间安全具有重要意义，包括：

- 全球互通。各国应在本国管辖范围内积极作为，确保互联网的端对端互通能力，使之成为所有用户均可访问的网络。
- 网络稳定性。各国在配置自身网络时，应尊重信息的自由流动，保证不对国际互联网基础设施随意干扰。
- 可靠访问。各国不可随意剥夺或妨碍个人用户访问互联网或获取其他网络技术。
- 利益攸关者共同治理。网络治理权不应仅限于政府，网络治理的参与者应包括所有具备资质的利益攸关者。

- 稳妥处置网络安全。各国应充分认识和履行自身保护信息基础设施的责任，并确保本国系统不被破坏或滥用。

由于网络空间是一个动态环境，网络空间国际行为必须以国家治理、和平开展跨国活动以及可靠的网络管理为基础。随着相关理念的发展，美国将致力于培育和全面参与相关讨论，推动互联网政策的合理制定，并促进各国在诸多事务上的共同理解。

（二）未来美国在网络空间中的角色

为实现这一愿景和推动良好规范的形成，美国将综合运用外交、国防和发展手段，以促进繁荣、提升安全、增加开放，使所有国家共同从网络技术发展中受益。在我们的国际努力中，有三项措施至关重要。20 世纪下半叶，在美国的帮助下，全球建立起了新型的国际经济和安全合作架构。在 21 世纪，我们将一如既往地秉持合作精神，承担共同责任，致力于打造一个和平、可靠的网络空间。

1. 外交：加强伙伴关系

将和平与安全的原则推广到网络空间——同时维护网络的优点及特性——要求我们加强伙伴关系并扩大努力范围。我们将积极与国际社会开展坦率和必要的对话，就网络空间负责任行为的原则和有必要采取的行动等问题，形成国内、国际共识，以建立一个稳定的网络体系。

加强伙伴关系。我们将通过外交和联盟关系，寻求将尽可能多的利益攸关者纳入这一网络空间构想中来，因为这将产生巨大的经济、社会、政治和安全效益。与国内外的民营部门开展富有成效的合作，将对我们的努力起到支撑作用。

分布式系统需要分布式应对，没有任何单独的机构、文件、安排或手段能够包办我们在网络化世界中的所有需求。从最终用户、民营硬件和软件销售部门、网络服务提供商，到地区性、多边性和包含众多利益攸关者的组织，都可能在网络功能开发方面扮演重要角色。

在国际竞争领域尤其如此，各国在维护和平与稳定、鼓励创新、维护经济和国家安全利益、保护与促进公民个人权利方面，发挥着长期作用。美国将在国际关系层面，致力于打造一个符合国际期望的环境，以稳定外交和防务政策，改善对外关系。

双边和多边伙伴关系。我们将与有关国家开展双边协作，合作处理对我国政府和人民具有重要意义的网络空间事务。我们必须首先谋求与持相近观点的国家一起，签订含义清晰的协定，并以此为出发点，扩大国际社会对网络空间行为规范的理解。我们将寻求进一步拓展伙伴关系，包括在全球范围内与各国各级政府一起，就网络空间事务开展广泛的双边对话。我们将与各国基于已有的成功执法经验，共同应对网络空间不断出现的各种挑战。此外，我们将积极与发展中国家保持接触，倾听它们对网络空间事务的意见。

国际组织和包含众多利益攸关者的组织。地区性组织在处理其成员国对网络空间安全所关注的问题上，已发挥出有效作用。这些组织在制定和实施行为规范方面，将发挥日益重要的作用。我们将继续利用自身在这些国际组织以及更大范围的国际组织中的成员地位，制定符合各组织专业特点、可实现各成员现实利益的建设性议程。在互联网治理方面，我们已采取重要措施，以确保自己在重要国际组织中的代表性。美国对相关国际努力保持敬意，并将继续重视有关论坛的特殊作用，这些论坛通过接纳民营部门、民间团体、学术机构以及政府

成员，体现出有众多利益攸关者参与的特点，切实代表了整个互联网社会。

与民营部门开展合作。虽然民营部门已经在国际性组织和包含众多利益攸关者的组织中扮演重要角色，但我们仍有必要进一步充分扩大已有合作机制，将更多产业部门纳为伙伴。尤为重要的是，我们应与基础设施产权拥有者及运营商——它们肩负确保网络正常运行的主要职责——紧密合作，以拓展努力范围，确保网络生态系统安全，保持网络空间的优点及特质，消除不必要的技术发展障碍，并将和平与安全原则推广至网络空间。我们还将寻求民营部门共同参与网络治理，以顺应网络空间存在众多利益攸关者的固有特质，并将继续在有关论坛倡导包容性。

2. 防务：劝阻及威慑

无论所面临的威胁来自恐怖分子、网络罪犯，还是国家或其代理人，美国都将维护自身网络安全。重要的是，我们将鼓励守法者，劝阻并威慑那些在网络空间中肆意妄为、威胁和平与稳定的行为者。我们将采取多项政策，结合国内和国际网络的恢复能力与警戒能力，并伴以多种可信的应对手段，来实现防御目标。在防御努力中，我们将根据自身法律和原则，保护民众的自由及隐私。

（1）劝阻。

保护这种高价值网络需要强大的防御能力。美国将继续加强网络防御以及抵御扰乱和其他攻击并进行恢复的能力。针对那些确实造成破坏的更为复杂的攻击，我们将依据周密的反应计划采取行动，隔离和削弱对我们机器的干扰，限制对我们网络的影响及潜在的后续影响。

- 国内实力。确保网络和信息系统的复原能力，要求举政府之全力，与民营部门和公民个人协作，采取全国性的协调一致的集体行动。十年来，美国政府一直在营造一种网络安全文化和一个化解风险与应对事件的有效机制。我们继续强调，在公共和民营部门系统性地采用合理的信息技术规范，将会减少我国的薄弱环节并增强网络和系统。我们还在公共和民营部门网络之间分享关于网络弱点和风险的信息方面取得了扎实的进展。我们已经通过国家计算机事件应急响应小组建立了在政府、重要企业、关键性基础设施部门和其他利益攸关方之间共享信息的新计划。我们不断探索加强与民营部门伙伴关系的新途径，以增强我们双方依赖的系统的安全。
- 国外实力。这种防御模式已经通过教育、训练以及日常业务交流和政策联系在国际上被成功共享。今天，通过技术和军事防御领域现有和发展中的协作关系，有关国家共享的识别和应对事件的能力达到了前所未有的程度——这关键的一步，将使潜在的攻击方无法获取对我们国家网络和国际网络施加持续性危害的能力。然而，全球分布的网络需要全球分布的预警能力。我们必须继续生成新的全球范围内应对计算机安全事件的各种能力，并为上述能力之间的相互衔接和计算机网络防御的强化创造便利条件。美国在帮助较不发达国家建设防御能力方面与我们的伙伴具有共同利益，因此将加强这方面的协作和投入。与盟友建立关系将增强国际社会的集体安全。

（2）威慑。

美国将确保攻击或利用我方网络所带来的风险远远超出潜在的收益。我们清醒地认识到，网络空间活动会产生超越网络范畴的效应，这种事件要求做出自卫反应。同样，互连的

网络将各国更加紧密地联系在一起，因此对一国网络的攻击会产生超出其国境的影响。

针对那些可能威胁我们国家安全和经济安全的犯罪分子及其他非国家行为体，国内方面要求各国具备相关程序调查、逮捕和起诉非法入侵或扰乱国内外网络的人员。在国际方面，各国执法部门要尽可能相互协作，对容易丢失且对当前调查起关键作用的数据进行固化处理，并与各国立法和司法部门合作，协调这些部门的手段运用，以推进应有的程序和法治——这些都是《布达佩斯惩治网络犯罪公约》的主要准则。

必要时，美国将像应对其他任何威胁那样应对网络空间的敌对行为。各国都有固有的自卫权，并且我们认识到，通过网络空间实施的某些敌对行为，将迫使我们根据对军事条约缔约伙伴的义务采取行动。我们保留根据国际法适当使用所有必要的外交、信息、军事和经济手段的权力，以便保护我们的国家、我们的盟国、我们的伙伴和我们的利益。在此过程中，我们将在动用军事力量之前尝试各种替代方案；我们将仔细衡量采取行动的代价和不采取行动的代价；我们的行动方式将反映我们的价值观并强化我们的合法性，在任何可能的时候寻求广泛的国际支持。

3. 发展：建设繁荣和安全

美国将继续展示我们的这一信念，即一个互连世界的利益是普惠的。一个开放、互通、安全和可靠的网络空间应惠及更多的人，作为世界领先的信息经济体，美国正致力于确保其他国家能从我们的技术资源和能力中获益。

我们的国家能够而且将会在提供建设和保护新的和现有数字系统所需的知识和能力方面发挥积极作用，并且在此过程中，在国家间达成共识以负责任的利益攸关者方式行事。建设实现这些目标的能力并非一项短期支出，恰恰相反是一项长期的明智投资，对于政府而言是一项继续参与的承诺。

建设技术能力。获取网络化技术越来越成为一项基本的发展需求。各国政府和企业已采取许多有意义的步骤，以实现网络接入的普遍化服务和充分服务。国际信息基础设施在不断走向成熟并继续扩展，为更多的国家提供融入全球信息流的机会。全球网络的发展以及网络访问能力的扩展，在丰富全球社会的同时，也产生了传统安全和网络安全问题方面新的挑战和协作机遇。网络安全能力的很大部分将来自民营部门的投资，美国将与各国政府和企业一道，营造有利于协作的环境，并利用这些协作解决各国核心的发展需求。

政府是最主要的决定因素，决定着此类新型互通是产生积极成果还是浪费潜在能力。从我们的能力建设中受益的国家，是那些利用技术促进繁荣和加强社会凝聚力的国家，而不是出于政治目的实施严格接入控制的国家。从上述原因出发，美国所支持的技术项目，在设计上将体现增强安全、促进商业、保护信息的自由流动，并提升全球网络的互通性。

建设网络空间能力。繁荣不能建立在恐惧和缺乏可靠性的基础之上，美国承诺致力于帮助建设网络空间能力，使其与国家技术发展同步。增强发展中国家的国家层级网络空间安全，具有当前和长远利益。当前，越来越多的国家正在准备，以应对来自边界内部的威胁。下一步要做的是，在全球互通网络中建立信任并开展跨国合作，打击滥用信息技术和信息犯罪。不可或缺的一点是，要充分利用国际研究界的力量，应对下一代网络安全挑战。

我们认识到网络安全是一个必须由所有国家共同努力加以解决的全球性议题，因此我们将扩展和规范那些着眼于网络安全能力建设的计划，将其关注点更多集中在培育感知能力、

提供法律和技术培训，以及支持政策发展方面。此类计划必须超越纯技术范畴，我们将与有关国家合作，使其充分认识到网络安全挑战的广度，帮助这些国家发展自身战略，并建立涵盖整个领域的能力——从网络安全和组建计算机应急战略工作组，到国际执法和防务合作，以及与国内、国际民营部门及公民社会发展建设性的关系。

建立政策关系。美国的能力建设援助被看做投资、承诺和拓展对话与伙伴关系的重要机会。在网络空间议题上，各国已成为利益攸关方，我们希望对话能够日益成熟，从能力建设，到在双方共同关注的领域开展积极的经济、技术、执法、防务与外交合作。对于那些发展网络安全能力的国家，我们将利用地区性论坛和具有特殊专业技能的技术实体，推动与其关系的发展。我们还将继续加强共享实践成果，共同总结经验，开展国际技术交流。

四、政策重点

美国将继续致力于在美国国内和国外，协助建立和维护开放、互通、安全和可靠的网络，为美国公民和国际社会的其他成员服务。我们的做法以本文阐述的基本原则为指导，以文中提出的总体目标为动力，并依据其概述的政策而行动——它们共同形成美国网络空间国际战略的基础。

在未来，网络的各种可能性将得到充分实现，服务大众。为实现这一愿景，美国政府在七个相互依存的领域开展活动，每个领域的活动都需要我们政府内部保持协调，并与国际伙伴和民营部门协作。

对于许多已经从事网络活动的美国政府部门和机构而言，它们的努力加强了这一进行中的重要工作。对于为执行特定网络空间任务而制定落实计划的部门而言，它们是本战略出台的背景，确保了行动的统一。本文提出的政策重点要求采取这些具体行动并对其提供指导，着重强调过去、当前及未来需要关注的重点领域，这些领域需要在国家层面予以共同的关注并投入资源。

（一）经济：推动国际标准和创新型的开放市场

为确保网络空间继续满足我们的经济需求和创新者的需要，我们将采取以下措施。

维护有助于对可靠、互通的网络进行技术革新的自由贸易环境。正如信息的自由流动对网络运行至关重要，自由贸易有助于信息时代的技术革新与市场增长。全球网络互通在很大程度上归功于低成本计算机在全球的普及和网络技术的传播。自由贸易环境使制造商努力保持低价高质，这种市场竞争是革新的动力。尊重技术进步和贸易方面的国际标准对于保持开放的市场必不可少，并使具有领先技术的公司能迅速将创新型的产品和服务转化为实在的收益。未来几十年，制造技术的全球化将不断增强，为我们的网络和消费者带来实质性的益处。美国将继续致力于维护自由贸易环境，特别是支持高科技行业，以确保在未来不断创新。

保护知识产权，包括防止商业秘密失窃。为创新提供动力的全球网络也为工业间谍窃取知识产权和商业信息打开了通道。通过网络空间可从商业企业、大学和政府部门窃取前所未有的海量信息。信息和技术失窃等同于损失数十亿美元。个别案例通常没有上报或未被注意，导致从不公平竞争到整个公司破产等一系列情况发生，还可能导致全国范围甚至更大规模的影响。犯罪分子、外国公司或实施国家行为的个体不断偷窃知识产权将削弱国际经济的竞争力，损害企业的创新机遇。美国将采取措施识别这类行为并做出反应，帮助建立国际环境把

此类行为视为非法并予以禁止，让行为者承担责任。确保技术专家所确定的互通、安全的技术标准占主导地位。制定国际性、自愿和公认的网络安全标准以及使用基于这些标准的产品、程序和服务，是建立互通、安全和富有活力的全球网络结构的基础。公共和民营部门必须共同合作，发展、保持并实行这些标准，支持制定国际标准及行为遵循评估计划，防止对国际贸易和商业造成障碍。国际网络安全标准和基于自愿、各方公认的程序，有利于实现整体利益。这些标准和程序有助于创新，便于网络互通、安全和加强适应性，提升网上交易可信度，并为全球市场提供动力。美国政府将与公共和民营部门合作，确保基于国际标准的产品和服务的普及。

（二）保护网络：加强网络安全性、可靠性和恢复能力

网络安全对于国家及经济安全至关重要，因此我们将采取以下措施。

推动在双边及多边组织和多国合作伙伴关系框架下的网络合作，特别是在各国网络安全行为准则方面的合作。越来越多的国际组织正在从事网络安全活动和其他网络空间事务，美国政府将继续推动这项重要工作，建立涉及这些组织的网络空间，满足不同成员国的需求。我们努力在以下多边框架内开展网络合作活动：美洲国家组织、东盟地区论坛、亚太经合组织、欧安组织、非盟、经济合作与发展组织、八国集团、欧盟、联合国和欧洲委员会等，并努力确保这种网络活动得到有效的机制框架的支持。美国政府将继续通过这些组织和其他平台，加强对于关键网络空间活动，包括有关行为准则的地区与国际共识。我们将依靠有助于各利益攸关方合作和达成共识的平台，进一步细化本文所阐述的网络政策原则。我们欢迎在本次对话中未得到充分体现的地理区域——主要是非洲和中东——加入我们的工作，以推动我们建立全球网络能力的努力。

减少对美国网络的侵入和破坏。未经授权的网络入侵对经济和国家安全造成损害。美国政府各部门正与民营部门合作，保护技术创新免受工业间谍的侵害，保护联邦、州和地方政府网络，保护军事行动免于不利的作战环境，保护关键性基础设施不受网络侵入和攻击，特别是防止对能源、交通、金融系统和国防工业基地的入侵和攻击。美国将努力达成广泛的国际共识，使各方认可尊重知识产权和网络稳定的重要性，并与我们的伙伴共同支持这一信念，保护我们的网络不受侵犯。

确保信息基础设施具有强有力的事件反应能力、适应能力和恢复能力。在互通的全球环境下，一个国家在系统上的安全弱点使其他国家面临的威胁复杂化。没有一个国家对世界网络有百分之百的了解。我们有义务分享对于网络的见解，就可能对我们造成共同威胁的情况进行合作。在致力于建立并增强我们反应能力的同时，我们将继续与其他国家合作，拓展有利于增强全球态势感知能力和事件应急反应能力的国际网络，包括建立政府与工业间的网络。美国政府通过与可信赖的国际伙伴交换信息，积极参与网络监控、网络预警和网络事件应急反应。我们将通过国际合作拓展这些能力以增强整体适应能力。美国也将积极参与国际网络安全演习，与伙伴共同提升和完善已确立的运作程序。

与产业界磋商，提升高科技供应链安全。关键性网络和信息基础设施的正常运转依赖于可信赖的软件和硬件的有保障的供应。供应链的弱点会被用于攻击网络和其中的数据，使网络的完整性、可用性和保密性受到影响。利用这些弱点会对经济运行和国家安全造成损害。美国政府将与产业界和国际伙伴共同努力确立最佳做法，保护信息系统和关键性基础设施不

受侵害。通过这种方式，我们将极大地增强自由和开放的贸易所依赖的全球供应链的安全。

（三）执法：拓展合作与加强法治

为加强网络空间领域的信任，招揽那些有能力发挥在线系统作用的人才，我们将采取以下措施。

全面参与制定打击国际网络空间犯罪政策。美国承诺积极参与旨在制定打击网络犯罪政策的国际准则与措施的双边与多边讨论，参加那些专业性得到证明、在有效推动制定打击网络犯罪政策方面具有实践经验的论坛。这些对话交流活动将包含现有工作，如扩大《布达佩斯公约》机制覆盖范围等。国家执法机构与富有成果的政策对话之间，已成功建立伙伴关系并使我们受益，在此基础上，美国将开展工作，努力在加入上述机制的国家中培育责任感。

通过增加布达佩斯会议成员国，协调国际网络空间法律。在调查和起诉网络犯罪案件时，美国及其盟友通常依赖其他国家的合作与援助。当这些国家拥有共同的有助于证据共享、引渡和其他种类合作的网络空间法律时，这种合作最为有效，也最具实际意义。“布达佩斯网络犯罪会议”为不同国家提供了草拟和修订当前法律的模本，也证实该会议是网络空间领域内提高国际合作的有效机制。美国将继续鼓励其他国家成为会议成员国，并将帮助当前的非会议成员国以会议（章程）作为其自身法律的基础，在短期内减轻双边合作的压力，为成为会议成员国做长期准备。

网络空间法律将集中打击非法活动，而非限制接入互联网。对网络空间的犯罪行为，应当实施有效的执法，而不是制定政策禁止合法接入互联网或限制互联网上的内容。为达成这一目标，美国政府通过双边和多边合作，确保这些国家认识到针对网上犯罪的努力应集中于防止、抓捕和惩罚犯罪分子，而不是泛泛地限制接入互联网，以免连累无辜的互联网用户。当美国及其伙伴进行对话并在世界范围内协助执法机构建设上述能力时，我们将协调这一方法，共同保护个人隐私和基本自由，创新合作以打击网络犯罪。

剥夺恐怖分子和其他罪犯利用互联网实施行动计划、筹措资金或发动攻击的能力。在对付网络犯罪方面，美国拥有多种国际能力建设和训练项目，帮助执法与立法者建立有效的法律框架机制和培养专业人才，以调查和起诉恐怖分子及其他犯罪分子对互联网的滥用。对国际社会而言，阻止恐怖分子通过“雇用黑客”和使用有组织的犯罪工具来增强犯罪能力是最重要的内容，同样需要有效的网络犯罪法律。美国承诺通过技术手段和像“资金行动特遣队”这样的国际合作框架，追踪和挫败恐怖分子及网络犯罪的资金网络。

（四）军事：准备应对 21 世纪的安全挑战

为了将我们保卫公民、盟友和利益的承诺延伸至任何遭受威胁的地方，我们将采取以下措施。

理解并适应军队对可靠与安全网络与日俱增的需求。我们认识到，我们的军队越来越依赖向其提供支援的网络，我们将努力确保军队使用精良的装备作战。即使在一个其他国家可能企图毁坏我们的军队网络系统或毁坏其他对国防至关重要的基础设施的环境中，我们也将努力确保其拥有精良的装备。与所有其他国家一样，美国在保护其重要国家资产和核心原则与价值观方面，有着不容忽视的巨大利益。我们承诺将击败那些企图削弱我们上述能力的敌人。

建立和提高现有的军事联盟以应对网络空间的潜在威胁。任何一个国家都无力单独实现网络安全，需要更密切的国际合作来挫败那些企图破坏或利用我们网络的行为。这首先需要认识到，我们与像北约这样的亲密盟友之间的网络连通，既创造了机遇，也带来了新的风险。美国未来将继续与盟友的军队和地方部门一道，增强我们的态势感知和预警情报的共享能力，提高危机与平时的协作水平，发展网络空间的集体自卫手段。这样的军事联盟与伙伴关系将增强我们的集体威慑力及挫败国家性质和非国家性质行为的能力。

扩大与盟友、伙伴的网络空间合作，增强集体安全。网络空间的挑战也创造了与盟国及伙伴国进行新式军事合作的机遇。通过强化对标准作战行动程序的共同理解，我们的军队能够通过协作和更多的情报交换来增强安全。这些协作将减少对军事活动的误判以及升级行为的可能性。对话和交流有助于提高伙伴国的能力，如数字法医学、劳动力培养、网络渗透和恢复能力测试等。为了震慑网络空间的恶意活动，美国将与盟友国家密切协作，以增强能力、减少集体风险并强化多利益攸关方计划。

（五）互联网管治：推动有效和包容性的管治结构

为了推动有效和包容性的管治结构，有效地满足所有网民的需求，我们将采取以下措施。

重点推动互联网的开放与创新。在互联网上有效分发信息的能力，对现代消费者、商业、政治、科学及教育活动等至关重要。各国政府都认识到互联网的价值，但很多国家随意限制信息的自由流动，或利用互联网镇压异见者和反对活动。在不同国家，这种限制手段迥异，借口也各不相同。但我们不能允许网络管治和技术手段被用来破坏最基本的自由，或抑制创新。有效和包容性的管治有助于确保超出国际规范的行为不会因技术或管治而变得复杂化。保护、提高和增加对公开的全球互联网的使用是一项地位优先的透明政策。美国将通过各种各样的合作，包括扩大至合适的多利益相关方机构或组织、相关政府和非政府机构等，来推动实现这些目标。

保持包括网络域名系统在内的全球网络空间的安全与稳定。考虑到网络对于世界经济的重要性，维持包括网络域名系统在内的全球网络空间稳定与安全非常必要。为确保这种稳定与安全的连续性，我们应与世界各国，特别是相关组织和网络技术专家一起，继续重视各利益攸关方在该领域发挥的重要作用。美国认为，在网络空间领域，各方力量与资源的有效协调运用，是互联网取得成功的重要因素。美国将继续支持这种有效的多方协调工作。

促进并加强各利益攸关方商讨互联网治理问题。互联网的框架结构包含既分散又合作的社会各层面和技术组织。这一特点是互联网为我们带来各种效益的基础。互联网的框架结构鼓励自由创新，并由此促进经济增长。互联网还鼓励言论自由和结社自由，以促进社会、政治发展，并使世界各民主社会表现出生机与活力。美国坚持认为，在国际社会共同探讨互联网治理问题时，必须有各利益攸关方共同参与；我们将继续支持诸如“互联网管理论坛”的成功举办。该论坛允许非政府利益攸关方参与平等讨论，使论坛在互联网问题上的探讨更具开放性和广泛的代表性。

（六）发展国际合作：提高能力，确保安全，促进繁荣

为促进全球网络技术的快速发展，加强网络运行的可靠性，构建网络空间各利益攸关方的责任机制，我们将采取以下措施。

为寻求提高网络技术与网络空间安全能力的国家提供必要的知识、培训和其他资源。一个相互连通的世界所带来的各种利益不应受到国界的限制。十几年来，为缩短在提高网络空间技术和安全的核心能力方面的差距，美国已制定许多项目，帮助一些国家获得了相关资源和技能。目的就是帮助别的国家学习我们的经验，特别是在技术开发过程中提高网络安全能力。鉴于需求较多且种类繁杂，我们的援助项目包括：支援事故管理能力，建立政府与免检伙伴关系，加强控制系统安全，制订调查和起诉网络犯罪的法律草案，制订并实施网络安全认知计划，建设国家网络安全文化。我们已经通过对外援助，并以公私伙伴关系计划的形式启动双边合作，如已开始实施的“美国电信训练学院”计划等。近年来，我们还在多边框架内，如在“美洲国家组织”、“亚太经合组织”和联合国框架内优先安排这项工作。美国将会进一步发展这些计划，与其他国家一起支持相关民营投资，关注相关重要需求，努力在未来几年内制订新的合作计划。

继续创造和分享国际网络空间安全的经验与技术标准。当前，各国已不再需要通过反复试验的方式来独立发展网络空间安全能力。我们已经开始与 12 个国家和众多多边组织合作，改进并分享相关网络安全实践经验，帮助这些国家合理投资，制订更有效的政策。美国将继续确认并优化相关实践经验与技术标准，加强合作伙伴关系，促进相关技术标准的认知和使用。我们将进一步促进相关科技研发合作，进一步加强网络空间安全手段建设，提高网络空间的安全保障能力。

增强国家打击网络空间犯罪的能力，包括提高执法能力，培训执法专家、法官和立法人员。由于涉及计算机网络的犯罪案件经常牵涉国外取证和目标认定，各国政府在遇到各种严重犯罪和国家安全问题时，经常需要相互帮助，提供各种技术并协助调查。各种犯罪威胁可能会发生在任何一个国家，更多的国家需要为此提供相关协查帮助。针对这些问题，我们可以通过相关培训加强联系，从技术层面获得各国执法部门的理解与支持，促进各国执法部门的有效合作与相互帮助。为实现这一目标，美国将继续在非洲等地区，以及在“亚太经合组织”、东盟、“八国集团”和“美洲国家会议”等多边组织内提供相关培训。

与政策制定者改进关系以加强技术能力建设，与专家及他国政府相应对等机构进行经常性沟通。过去几年，各国越来越多的政策制定者关注网络空间问题。这为对话提供了渠道，帮助启动了新的安全与发展倡议，并加强了众多双边关系。美国在发展中国家开展了长期投资，其中包括技术和网络安全能力建设方面的投资。美国愿在彼此关切的问题上将援助关系发展成更亲密的伙伴关系。美国在召集国际子午线会议（该会议推动了在关键信息基础设施保护问题上的合作）等方面扮演了领导角色。由于更多国家正加大对未来网络空间的投资，美国欢迎各国加入对话，并与美国专家和政策制定者建立持久联系。

（七）互联网自由：确保基本自由和隐私安全

为确保网络空间的基本自由和隐私安全，美国将采取以下措施。

确保公民通过可靠、稳固和安全的平台自由发表言论与结社。鼓励世界各国人民通过数字媒体表达观点、分享信息、监督选举、揭露腐败、组织社会和政治运动。公开谴责通过骚扰、非法逮捕、威胁或使用暴力等行为来反对利用这些技术的人，上述行为阻碍了其他人利用新技术报道消息、组织活动和交换观点。这种保护必须同样适用于互联网运营商和其他提供接入服务的商业机构，它们经常沦为受害者，因为一些政权往往会将审查合法言论的职能

赋予企业。美国将不遗余力地推动网络空间中的言论自由和结社自由；努力使公民社会参与者、人权推动者和记者都能使用数字媒体；将致力于鼓励各国应对现实网络威胁，而不是强制商业公司不合时宜地限制网络言论自由或信息的自由流通。

与公民社会和非政府组织合作，建立安全措施，保护网络活动免受非法侵扰。保护公民社会和非政府组织的网络安全，可帮助确保数字时代享有更广泛的言论和结社自由。网络安全对那些身处一线、表达不受欢迎的观点和想法的社会活动家、倡导者和记者尤为重要。他们往往是受害者，他们的电子邮件账户、网页、手机和数据系统经常受到破坏和侵扰。美国支持相关努力，以使此类用户有能力自保，并确保他们利用 21 世纪的新技术行使他们的言论自由和结社的权利。

鼓励国际合作，有效保护商业隐私数据。保护个人隐私对维护信任至关重要，正是这种信任维系着经济和社会网络。美国在贯彻其隐私保护法、鼓励多利益攸关方政策发展方面记录良好。我们将紧跟网络技术带来的急剧变化，继续加强美国的商业隐私数据保护框架。我们认为，在商业领域应用普遍隐私保护原则的同时，保持创新所需的灵活性也十分重要。美国将努力使达成这一目标的相关法律得到各国共同认可，并在保护隐私和促进创新方面加强合作。

确保端对端网络的互通性，确保人人都能使用网络。网络用户应相信，他们通过网络发送的信息在世界任何地方接收时仍能保持原意。同样重要的是，他们应相信，不管这些数据来自哪个国家、目的地又是何处，都将在网络上自由流通。确保信息在网络中流通时的完整性，将使用户对网络充满信心，并可保持网络的开放性，使其成为一个推动全球经济增长创新、鼓励世界各国人民自由交流的可信平台。美国将继续确保互联网的全球属性带来的益处，并反对任何试图将互联网分裂为一个个国家内部网络的努力。

五、继续前进

网络技术的益处不应为少数国家独享，或者为少数人独享。但互联网的连通性本身并不是目的。互联网必须是一个有利于创新、全球互通、足够安全以赢得公众信任、足够可靠以支撑公众工作的网络空间。

30 年前，很少有人能够理解被称为互联网的东西将推动我们工作和生活方式的变革。短短 30 年后，已有数百万人靠网络技术谋生，约十亿人通过它进行日常社会交流。这种技术推动了社会进步，使前几代人难以想象的事情得以实现。对我们来说，美国将继续激发美国人民乃至全世界人民的创造力和想象力。我们不知道下一项伟大创新将会是什么，但我们将致力于创造使其得以产生和发展的环境。

本战略是一个路线图，它使美国政府各部门和机构可以更好地界定和协调其在我们的国际网络空间政策中的角色，按照特定的路线前进，并对未来如何贯彻该战略进行规划。它还是一种号召，号召所有民营机构、公民社会和终端用户在合作、意识和行动各方面加强努力。更为重要的是，它是一种邀请，邀请其他国家和人民与我们一道，实现我们所处的网络化世界的繁荣、安全和开放的美好前景。这些理想和目标对于保护我们已认知的网络空间，以及共同创造我们追求的美好未来都是至关重要的。

网络空间行动战略

网络空间是现代生活的标志。世界各地的个人和团体都能借助网络空间彼此联系、相互结识和组织管理。2000—2010 年，全球互联网用户数量从 3.6 亿跃升至 20 亿。随着全球互联网用户的进一步增加，网络空间将日益成为日常生活的重要组成部分。

美国和世界各地的商业部门利用网络空间交易商品和服务，在转瞬间实现全球的财富转移。在推动其他领域贸易活动的同时，网络空间自身也成为全球经济的一个至关重要的领域。网络空间催生了新的企业部门、科技进步、自由言论传播，以及新的社交网络，这些新事物推动了经济的发展，体现了我们国家的原则。美国关键基础设施的安全和有效运作，依赖网络空间、工业控制系统和信息技术，但它们却极易遭到破坏和非法侵入。这些基础设施包括能源、银行金融、运输、通信以及国防工业基地等。

美国国防部和政府其他部门履行职能依赖网络空间。这种依赖性显而易见，国防部在全球几十个国家的数百个设施内，拥有 1.5 万个网络和 700 万台计算机。国防部利用网络空间开展军事、情报和商务活动，包括人员和物资的调配，以及各种军事行动的指挥控制。

军队和国家在网络空间领域存在诸多薄弱环节，对网络空间的依赖与网络安全的不完备形成了鲜明对比。而且，网络化系统、设备和平台数量的持续增长意味着，网络空间日益融入国防部赖以完成其使命的多种能力之中。当前，许多国家致力于非法侵入国防部保密和非保密网络，一些国外情报机构已经具备了破坏国防部信息基础设施的能力。更为严重的是，非国家行为体日益威胁侵入和破坏国防部的网络系统。我们确信，大量针对国防部网络系统的恶意行动尚未被发现。

国防部与其他机构和国际合作伙伴一道，致力于减少美国和盟国网络空间能力面临的危险，并致力于保护和尊重个人隐私、公民自由、言论自由和改革创新，这使网络空间成为美国繁荣和安全不可分割的组成部分。未来几年，国防部是否能够既抓住网络空间带来的机遇，又能有效管理网络空间内在的不确定性，并减少薄弱环节，将极大地影响美国的国防战备和国家安全。

一、国防部在网络空间的能力与机遇

国防部，乃至整个国家都需要一个安全可靠的网络空间，以保护最基本的自由、隐私和信息畅通。国防部在网络空间领域拥有强大的能力和重要机遇，能够支持国家履行核心义务，提升国家安全。美军借助网络空间快速通信和信息共享能力支援作战行动，是国防部至关重要的能力。换句话讲，国防部在全球信息与通信技术领域的研究成果，包括网络安全专家力量，为国防部提供了在网络空间领域中的战略优势。

美国公共和民营部门的人力资源和研究成果，为国防部提供了建立当前和未来网络空间能力的雄厚基础。通过在人员、研究和技术方面的投入，国防部在建立和利用美国民营部门技术力量方面，发挥了重要作用。国防部将继续推进与企业的合作，与这些团体和机构合作成功开展网络空间活动。网络空间不断发生变化，这就要求不同国家间应开展合作，以保护

其共同利益和安全。国防部与盟国及其他国际合作伙伴的合作关系，为未来美国国际安全合作提供了坚实基础。连续的国际合作、集体防卫以及国际网络空间规则的建立，将强化网络空间安全，并使各方受益。

二、网络空间威胁

互联网具有协作性、快速扩展性，以及对技术创新的适应性。信息流动比信息完整更加重要，实现互联远比身份认证重要。互联网对国防部及其军事行动的作用不断增加，这一点互联网的最早设计者们恐怕没有想到。另一方面，国防部在全球范围内的网络系统，也给对手提供了大量非法入侵和恶意攻击的机会。

实施恶意网络行为的门槛低，其中包括黑客工具随处可得。这意味着由个人或小团体组成的网络行为主体一旦下定决心，可能会对美国国防部与国家和经济安全造成重大破坏。小型技术可产生与其规模不成比例的效果，潜在敌手不必因试图对美国国家安全构成重大威胁而制造价值不菲的武器系统。

在制定网络空间行动战略的过程中，美国国防部重点关注网络威胁的诸多核心环节；这些环节包括外部威胁行为主体、内部人员威胁、供应链脆弱性，以及美国国防部行动能力所面临的威胁。美国国防部必须设法消除弱点，防止国家与非国家行为主体采取协调行动，图谋未经授权进入其网络和系统。

来自国外针对美国公共和民营部门系统的网络空间行动数量不断增加，手法更趋老练。美国国防部网络系统每天遭到数百万次刺探，美国及其盟国和行业合作伙伴因遭受网络入侵，已造成数以千计的文件失窃。此外，这一威胁甚至愈演愈烈，因为有越来越多的证据表明，敌人正致力于发展技术水平更高、潜在危险性更大的能力。

小团体具备在网络空间产生非对称效应的潜力，从而为恶意行为构成非常现实的诱因。除正式的政府行为外，网络犯罪分子可利用数百万台受感染的主机控制网络节点。网络犯罪分子正以令人难以置信的速度不断提高其网络工具和技术的先进性，这些技术大多可在国际互联网上低价购得。无论其目的在于赚钱牟利、获取知识产权还是破坏国防部关键系统，迅速演变的威胁态势都会对国家和经济安全构成复杂而严峻的挑战。

某些网络空间威胁还可能来自内部人员。心怀不轨的内部人员可能会听命于外国政府、恐怖组织、犯罪分子或出于自身目的，滥用其进入网络的权利。他们无论是从事间谍活动、发表政治宣言，还是表达个人不满，都会对国防部与国家安全造成极具破坏性的后果。

软件与硬件在被整合为操作系统之前就有遭受恶意篡改的风险。用于美国国内的信息技术产品大多在国外生产与组装。国防部依赖国外生产与研发的信息产品，在有关设计、制造、服务、销售、使用等环节的风险管理上构成挑战。

美国潜在敌手可能试图利用、破坏、阻止、损毁美国国防部赖以采取行动的网络和系统。美国国防部尤其关注潜在敌对行为的三大领域：一是窃取或非法利用数据；二是破坏或阻止入网或可影响其使用网络、信息或网络能力资源的服务；三是采取包括恶化、操纵或直接威胁、破坏或损毁网络及相关系统在内的毁伤性行为。

美国国家安全面临的网络威胁远非仅限于军事目标，还涉及社会的方方面面。黑客与外国政府利用尖端技术手段，侵入关键性民用基础设施，控制网络和系统的能力正在不断增强。由于网络空间具有综合性，因计算机导致电网、运输网或金融系统发生故障，将造成重大的

物理破坏与经济崩溃。美国国防部在国内外采取的行动均有赖于这一关键性基础设施。

与关键性基础设施所面临的威胁相比，知识产权面临的威胁虽然不够直观，但如今却是最具渗透性的网络威胁。每年都有大量知识产权通过美国各行业、大学、政府部门和机构所维护的网络被盗取，数量远大于国会图书馆。由于军事实力最终取决于经济活力，知识产权持续受损势必殃及美国的军事效能，以及其在全球经济中的国家竞争力。

三、五大战略计划

（1）战略计划一：将网络空间作为与陆、海、空、太空并列的“行动领域”，对美军进行组织、培训和装备，以便国防部能充分利用网络空间的潜能。

尽管组成网络空间的网络与系统是人造的，通常由私人拥有并主要供民用，但是将网络空间视为一个领域是国防部履行国家安全使命的一个关键组织概念（Critical Organizing Concept）。它允许国防部对网络空间进行组织、培训和装备，就像我们在天空、地面、海洋、太空中所做的那样，以支持国家安全利益。而且，这些工作必须考虑到在恶化的网络环境中履行基础使命的情况。

正如《国家安全战略》中指示的，国防部必须确保有足够的能力在海、陆、空、太空和网络空间等所有领域开展有效行动。国防部将在每一层面上组织、培训、装备，并迎接网络空间复杂的挑战和巨大的机遇。为此，国防部部长已将网络空间的使命分配给美国战略司令部（USSTRATCOM）、其他作战司令部（Combatant Command）以及军事部门。鉴于有必要确保在网络空间中有效行动及有效组织资源的能力，国防部成立了美国网络司令部（USCYBERCOM）作为美国战略司令部的次级联合司令部（Sub-unified Command）。网络司令部的成立反映了国防部的如下需求。

- 通过增加培训、信息保障，提升态势感知和创造安全、有弹性的网络环境等措施来管理网络空间的风险。
- 通过缔结明智的伙伴关系、打造集体自我防御（Collective Self Defense），以及保持对行动背景的共识来确保完整性和可用性。
- 通过与作战司令部、现役部队、各机构和采购团队（Acquisition Community）进行密切合作，快速传递和部署最迫切需要的创新能力，以保证综合能力的提升。

美国战略司令部已委托网络司令部负责同步和协调美军每一分支中的各个兵种组成部分，包括美国陆军网络司令部、美国海军舰队网络司令部/美国第 10 舰队、第 24 空军部队、美国海军陆战队网络司令部、美国海岸警卫队网络司令部。成立美国网络司令部背后的一个关键的组织概念是其与国家安全局（NSA）的协同定位。此外，国家安全局局长同时兼任美国网络司令部的司令。这些独立的不同机构间的协同定位和兼职使得国防部以及美国政府，能够最大化地利用人才和能力、发挥各自的影响力和更有效地行动，以达成国防部的使命。

由于长期恶化的网络空间行动可能成为事实，在完成任务的过程中可能会出现网络破坏，因此国防部将把各种网络空间假想情况整合到演习和培训中，以帮助美军为各式各样的偶然事件做好准备。这一行动的基石是将网络红军引入整个战争模拟和演习之中。在存在网络漏洞的前提假设下，国防部必须行动机敏、灵活，将重点放在任务保障以及关键行动能力的保持上。

这些努力将随着网络和系统的发展及不断增加的适应能力而得到有力的支撑。在涉及网

络故障或重大泄密的意外事故时，国防部必须通过隔离及压制其影响、使用储备能力或将行动转移到其他系统等措施，保持行动的有效性。多重网络能增加网络空间行动的多样性、恢复率及任务的成功率。国防部正在投入资金研究，能否将全部行动成批移植至安全网络。

（2）战略计划二：国防部将利用新的防卫行动概念来保护其网络和系统。

国防部现在和未来的网络空间任务的实现要求落实不断进化的防卫行动概念。第一，国防部正在加强其网络卫生（Cyber Hygiene）最佳做法，以提升网络安全。第二，为阻止、减少内部威胁，国防部将加强其员工交流、员工问责以及内部监控和信息管理能力。第三，国防部将利用积极的网络防御能力来阻止针对国防部网络和系统的入侵。第四，国防部正在开发新的防御行动概念和计算体系。这几部分内容共同构成了适应性强、具有动态防御能力的国防部网络和系统。

良好的网络卫生可以解决针对国防部系统的恶意行动及其多数漏洞。所有人必须时刻注重网络卫生。员工要像保护自己一样时刻保持安全软件和操作系统的更新。国防部将借鉴民营行业采用的不断更新的做法，强化其计算设备安全，坚持网络卫生最佳做法。良好的网络卫生将延伸到信息安全的维护、向用户与管理员推广网络安全最佳做法、安全的网络设计和实施，以及智能有效网络的部署和网络配置管理。这些措施将为国防部的网络和系统提供保护、监控、维护、设计和看管，以确保其安全性和完整性。

人是国防部维持良好网络卫生、减少内部威胁的第一道防线。为减少内部威胁、防止敏感的密级信息发生危险的泄露，国防部将加强并超越现行的信息保障模式，包括探索新的行动概念以减少漏洞。国防部将重点关注人员交流、人员培训以及新技术和流程。国防部致力于在员工内部树立更强的信息安全文化以确保个人履行其职责，通过加大对恶意活动的惩罚力度来修正员工的行为和态度，防止内部人员的恶意行为。这种文化的转变将由新政策、新的人事培训方式以及新的员工沟通方式来实现。

随着恶意网络活动的持续增加，国防部已经部署积极的网络防御（Active Cyber Defense）来阻止对国防部网络和系统的入侵并击退敌对行动。积极的网络防御是国防部同步、实时地发现、检测、分析、减少威胁和漏洞的能力。它建立在传统的国防部网络和系统的防御方式之上，并在新的行动概念指导下补充了最佳做法。由于无法保证每次都将恶意入侵阻断在网络边界以外，国防部会继续运行和改善其高级传感器，以监测、发现、定位和减少国防部网络上的恶意活动。

为增强网络和系统的恢复力及智能多样性，国防部将针对现有和新兴的挑战探索新的、创新性的途径和模式。这些努力将包括对移动媒体和安全云计算的开发和整合。国防部将不断调整在网络空间所做的努力，迎接快速演化的新挑战。

（3）战略计划三：加强国防部与其他政府部门、机构及民营部门的合作，以实现整体政府的网络安全战略。

来自网络空间的威胁横跨各部门、各行业以及美国政府的部门和机构，它们跨越国界，延伸到全球经济的多个组成部分。国防部的许多关键职能和运转依赖于商业资产，包括 ISP 和全球供应链，但国防部无权对这些资产进行直接干涉并有效减少其风险。因此，国防部将与国土安全部、其他跨机构伙伴以及民营行业共享思路，开发新能力，共同努力迎接网络空间的跨领域挑战。

为实现整体政府（Whole-of-government）之路，国防部将继续与跨机构伙伴在探索新的

和创新性的方式上密切合作，以提升国家网络安全。由国土安全部部长和国防部部长签署的有关共同合作和强化网络安全协作的 2010 年谅解备忘录就是一例。两者间更密切的合作关系将从三方面提升国家网络安全：第一，正式化的合作架构再次证明现行的法律和政策对国防部和国土安全部协作所设的限制；第二，双方联合参与项目规划将提高各部门的任务有效性，特别是它将提升双方对网络安全需求的共识，并确保隐私和公民自由受到保护；第三，备忘录将节约有限的预算资源。该备忘录将协助国土安全部最大限度地保护政府执行机构的.gov 域名，与各州、地方、部族政府以及民营行业共同合作，协调做好美国关键基础设施的防卫工作。

国防部还和国防工业基地（DIB）合作加强对敏感信息的保护。DIB 由公私组织和企业组成，它们通过提供国防技术、武器系统、政策和战略发展以及人员来支持国防部。为增强对 DIB 网络的保护，国防部在 2007 年成立了国防工业基地网络安全与信息保障（CS/IA）项目。在这个项目的基础上，国防部也正在试点建立一种政府与民营行业间的伙伴关系，目的在于展示主动共享有关恶意或非授权网络活动信息和网络安全保护措施的可行性与益处。

鉴于网络空间迅速变化的特点，国防部将继续与跨部门伙伴和民营行业一起审查新的网络安全协作方式。这些努力将包括国防部支持由国土安全部牵头，带动各机构确定并减少国家关键基础设施中存在的网络漏洞。要想取得成功，就需要推出更多的试点项目、商业模式和政策框架以培育政府与民营部门间的协作关系。建立政府与民间的伙伴关系要求双方在管制和自愿之间寻求平衡，这种伙伴关系将建立在创新、开放和信任的基础上。在一些情况下，激励手段或其他措施对于促进私人部门参与将十分必要。国防部的努力还必须从大企业扩大到中小型企业，以确保参与的广泛性和创新的有效利用。全国上下的共同协作将有利于找到解决政策问题的通用可行的方案，从而在增进网络安全的同时深化公众利益。

国防部将持续支持发展整体政府之路，对 ICT 领域的全球化风险进行管理。许多美国科技公司将软硬件的部分生产要素，有时甚至是知识库，外包给海外的公司。此外，假冒产品和部件的数量不断增长也要求采取一定程序以减少风险和提高质量。依赖来自不可信资源的技术无法确保国防部要求的可预见性和保障，国防部将与国土安全部及其跨机构伙伴一起更好地识别和应对这些风险。全球科技供应链对国防部企业的关键职能，以及美国政府和民营行业的核心功能产生影响，必须通过战略性的政府与民间合作降低其风险。

（4）战略计划四：打造与美国盟友及国际伙伴之间的坚固关系，强化集体网络安全。

在支持美国《国际网络空间战略》以及与跨部门伙伴的合作中，国防部将寻求日益稳固的国际关系，协助实现我们在网络空间的核心承诺和共同利益。国际共享的态势感知能力和预警能力的发展将形成集体自我防御和集体威慑。通过及时共享网络事件、恶意代码的威胁签名，以及有关新出现的行动者和威胁的信息，各盟友和国际合作伙伴的集体网络防御能力将得到提高。网络空间是一个网络的网络，它包括了遍布全球的成千上万家 ISP，没有一个国家或组织能够依靠一己之力保持有效的网络防御。

国防部的国际参与将有力地支持美国的《国际网络空间战略》以及总统就基本自由、隐私和信息自由流动所做出的承诺。国防部将协助美国推进国际网络空间的标准和原则的开发和改善，从而提升其开放性、互操作性、安全性和可信度。国防部将与跨机构伙伴以及国际伙伴一起鼓励负责任的行为，反对破坏网络和系统的意图，劝阻、威慑恶意行动者，保留在必要和适当的时候防御重要国家资产的权利。这些努力将保证在网络空间实现创新和利益共享。

随着国际网络空间合作的持续发展，国防部将推进其与盟友之间在网络空间的密切合作，捍卫美国和盟国在网络空间的利益。国防部将与其盟友和国际伙伴密切合作，发展共享的预警能力，加强能力建设，组织联合培训活动。这些合作将为在取证、能力发展、演习参与、政府与民间的合作等领域共享经验开启对话提供机会。而且，发展责任共担机制能增加各国的核心力量和能力，对那些欠熟练伙伴地区起到促进作用，增强能力和集体网络安全。

国防部将把正式和非正式的网络合作扩大到盟友和军事伙伴当中，以发展集体自我防御，增强集体威慑。国防部将为观点相近的国家创造新的机会，依据共同的原则协同工作。与盟友和国际伙伴之间扩大的、强化的关系能将不足的网络能力最大化，减少威胁，并为阻止网络空间的恶意活动创造各种形式的合作。这些合作将能够增加国防部的正式盟友和合作伙伴，并实现更广泛的网络安全。

（5）战略计划五：国防部将通过打造特殊的网络技术人才力量和快速的技术革新，提升国家的创新能力。

美国在网络空间的国家安全利益需要美国人民发挥才智和创新精神来捍卫。国防部将调动科技、学术以及经济资源，打造一个由平民及军人组成的人才库，执行网络空间的行动，实现国防部的目标。技术革新处于国家安全的前沿，国防部将鼓励快速革新并加强其采购程序，以确保有效的网络空间行动。国防部将在人员、技术、科技和研发方面投入资金，打造和维护对国家安全至关重要的网络空间能力。

发展并保持杰出的网络技术人才对于保障国防部在网络空间中的战略成功和本战略列出的每一计划的执行都很重要。国防部将定期评估其网络空间人才队伍、各项要求和能力。发展网络人才队伍对于国防部来说极为重要。

与网络威胁的严重性相对应的是，对新的网络人员的要求也很高。如果国防部想吸引技术熟练的人才为政府长期服务，就必须提高自身的竞争力。为此，国防部将重点专注于建立动态项目，以早日吸引到人才。国防部将利用“2010 年总统计划（Presidential Initiative）”来改进联邦招募和雇佣程序。国防部还将与“总统行政办公室”合作，探索各种策略以简化网络技术人才的招聘流程，设计政府与民意报告-行业之间的网络专家交换项目，允许实现人才“无惩罚”的交叉流动，以保持并培养创新型网络人才。

除了这些招募、教育和培训计划外，采用跨代的导师计划将为国防部实现未来的国防和国家安全任务培育一个网络天才库。范式转换（Paradigm-shifting）方式，如在预备役和国民警卫队发展网络能力，将在国防部、联邦、各州和民营行业活动中形成更强的能力、更高的专业水准和更大的灵活性。国防部将利用交流机会以及持续教育项目，融合企业的管理方式发展网络人才队伍。持续的教育和培训将成为网络人才的标志，从而保存和发展国防部的知识资产。

为借鉴民营行业的活力，掌控新兴计算理念的力量，国防部的信息技术采购程序将采用五大原则。

第一，速度是首要考虑因素。国防部的采购程序和管理必须跟得上技术发展的生命周期。对信息技术来说，采购周期应为 12～36 个月，而不是 7～8 年。

第二，国防部将采用渐进的方式发展和检验系统，而不是一次性部署大型的复杂系统。

第三，为了实现快速的渐进式发展，国防部愿意放弃或推迟一些定制功能。

第四，国防部的各种信息技术需求，从核指挥与控制系统的现代化到文字处理软件的更

新，将根据国防部对各种关键系统的优先级而采用不同的监督等级。

第五，国防部购买的所有系统，包括软件和硬件，都要采取改进的安全措施。不能存在有渗透风险的后门，不能留下活跃的测试模块。

这些原则将构成国防部的可信防御系统和供应链的风险管理战略，并将不断强化。至于所用的硬件、软件、结构、系统和程序，国防部将采取深层次的安全方式来设计、采购和实施可信赖的系统。

国防部还将增加中小企业的机会，与硅谷和其他美国技术革新中心的企业家一起将各种概念从创新性的想法快速推进到试点项目，进而推广至泛国防部的企业。国防部的网络空间采购项目将反映出网络空间的适应性本质，它强调灵活性，接受新的行动概念，并推动科学界和美国政府（作为一个整体）之间的协作。

国防部将利用改变游戏规则的方式（包括新体系），来强化国防部的防御能力，并使国防部的系统能够更加有效地抵御恶意活动。国防部将寻求革命性的技术，以对网络空间的技术基础进行重新思考。为此，国防部将与领先的科学机构合作开发新的安全可靠的网络空间能力，从而更好地抵御恶意活动。

国家网络靶场（National Cyber Range）的发展将推动国防部的上述和其他努力取得成功，它使得国防部、其他美国政府机构和潜在的美国政府以外的合作伙伴能够测试和评估新的网络空间概念、政策和技术。尽管美军定期针对目标靶场和模拟各种场景开展常规演习，但国防部在模拟网络空间行动方面的能力有限。国家网络靶场能够快速生成大量的网络模型，旨在帮助军方和其他部门通过模拟、检验新技术和能力来解决上述需求。

为鼓励民营行业参与稳健网络空间能力的发展，国防部将授权一些组织承担创新性概念和技术的交易所，并对那些开发出具有深远影响力和创新性技术的企业进行奖励。除了与知名的技术中心建立联系外，国防部将通过小企业革新研究（SBIR）、创新风险投资以及针对新兴和新概念进行的定向投资和拨款等方式，充分调动小型企业和创业者的创造力和灵活性。

美国的人才、技术和活力为国防部提供了建立军事和民用劳动队伍、提升技术能力的坚实基础。国防部将持续发展稳健的网络空间能力。国防部将在未来的人员和能力建设方面进行投资，以达成其网络空间目标，并支持美国的国家安全。

国家安全正在被网络空间重新定义。除了机遇，国防部还面临网络空间的严峻挑战。国防部的军事、情报和商业行动的成功都依赖于网络空间。《网络空间行动战略》对这些挑战和机遇进行了评估，并为国防部完成网络任务制定了一条战略途径。

国防部的五大战略计划为国防部提供了一份路线图，指引其在网络空间开展有效行动、捍卫国家利益和实现国家安全目标。每个计划都是独特的，但又与其他四个计划密不可分。纵观整个战略，在其中一项计划中所采取的行动都将有助于提升国防部的战略思考并为其他几项计划带来新思路。

通过执行本战略中的各项行动，国防部将充分利用网络空间提供的机遇，防止国防部的网络和系统受到入侵和恶意活动的攻击，支持跨机构、国际间和关键行业伙伴在提升网络安全方面所做的努力，发展稳健的网络空间能力和伙伴关系。该战略将指导国防部在网络空间捍卫美国利益，从而使美国及其盟友和合作伙伴能够继续从信息时代的创新中获益。

信息共享与安全保障国家战略

一、总统致辞

作为总统，确保美国与美国人民祥和安宁是我义不容辞的责任。完成这一使命需要我们的情报、军事、外交、国土安全、执法与公共卫生机构，以及我们在各州、各地方政府和民营部门的同行们尽可能地密切合作。同样，这种合作需要及时有效地把那些对我国构成威胁的相关情报和信息共享给最需要的人，从总统到街头巡逻的警察。

自 2001 年 9 月 11 日美国遭受恐怖袭击以来，我们看到美国在信息共享方面已经取得了长足进步。今天，我们的情报分析人员、调查人员以及公共安全专家正在共享更多的信息，开展相对于以前来说更加高效的合作。遗憾的是，我们仍存在一些不足，一些重要信息不能大范围迅速充分共享，一些机密或敏感信息在未经授权的情况下披露给外界，这损害了我们的国家安全。

为了保护国家安全我们需要共享信息，而且要保护这些信息不被其他人用于损害我们的国家，《2012 年信息共享与安全保障国家战略》的目标是要在这两者之间取得适当的平衡。虽然这两个重点——共享与安全保障——往往被人们以为是互相排斥的，但事实上，它们是相互促进的关系。

因此，此战略强调采取何种手段加强对于机密与敏感信息的保护，这有助于各参与部门与机构树立信心并在彼此之间建立互信，只有这样，这些信息才能在授权用户之间共享。

《2012 年信息共享与安全保障国家战略》认为重要信息是国家资产，必须受到保护并加以适当共享。美国的国家安全所面临的威胁不断发展变化，因此，我们的政策也要相应做出调整，确保重要信息得到有效使用与保护，达到预期效果。这包括保护美国人的隐私与个人信息，并坚持我们对于透明度的承诺。该战略明确指出：美国人的个人隐私、公民权利与公民自由必须而且应该得到保护。

我们的国家安全依赖于在合适的时间在适当的人群中共享正确无误的信息。因此，我们要努力工作，使信息可以在负责、无缝、安全的环境中共享。在此战略的指引下，我们将继续利用重要信息维护国家的安宁与同胞的安全。

巴拉克·胡赛因·奥巴马

二、执行摘要

我们的国家安全依赖于我们在合适的时间在适当的人群中共享正确无误信息的能力。这种信息共享授权需要联邦、州、地方、部落、领地、民营部门和外国合作伙伴彼此之间开展持续与负责的合作。过去几年，我们已经成功地理顺了相关政策与程序，克服了文化上的障碍，对信息系统更好地进行整合，使其能够在今天动态的作战环境中实现信息共享。不过，我们仍然面临着挑战，需要继续完善信息共享与信息安全保障的流程，并提高信息共享与信

息安全保障能力。技术上的不断创新增强了我们信息共享的能力，同时也增加了漏洞暴露的可能性，这要求我们强化信息安全保障工作。《2012 年信息共享与安全保障国家战略》为有效制订、整合并执行政策、程序、标准以及技术提供了指导意见，以促进安全与负责的信息共享工作。

我们必须具有战略眼光，立足于 3 项核心原则，这样才能应对这些挑战。首先，我们应把信息视为国家资产，认识到各部门和机构都已经达到了前所未有的能力，能够收集、存储并使用与它们的任务和适用法律职权相一致的信息；与之相应，它们有责任利用这些信息为完成国家安全任务提供支持。其次，我们开始确认信息共享与安全保障需要各部门与机构共担风险管理。为了建立并维持彼此间共享信息所需的信任关系，我们必须共同努力确定风险，并集体降低这种风险，而不是因噎废食，为了避免损失而根本不去共享信息。最后，从信息通报出发做出决策是核心前提，这是我们一切行动的基础，它提醒我们：更好地制定决策是信息共享的目的，要把这一观念摆在首位。

《2012 年信息共享与安全保障国家战略》侧重于实现 5 个方面的目标。

（1）通过协作与责任划分推动集体行动。

当我们共同努力，采用合适的管理模型使任务顺利完成，在可能的情况下采用通用流程建立起相互间的信任关系，简化信息共享协议制订过程，并且通过绩效管理、培训与激励机制为最终结果提供支持时，我们就可以更好地实现我们的共同目标。

（2）通过共同标准改善信息发现与获取的结果。

改善信息的发现与获取包括制订清楚的政策，使信息可供得到批准的个人使用。安全地发现并获取信息依赖于标识、身份验证和授权控制、数据标记、企业范围内的数据相关性、共同的信息共享标准，还需要有严谨的程序确认并验证其用途。

（3）通过共享服务与互操作能力，优化任务效能。

努力优化任务效能，包括共享服务、数据与网络的互操作能力，并提高采购的效率。

（4）通过结构改革、政策和技术解决方案强化信息安全保障。

为了提高信息的可信度并保障其安全，我们制定的政策和具体协调机构必须把工作重点放在识别、预防和减轻内部威胁和外部入侵上，同时各部门与机构要努力提高数据层控制能力、自动化监控能力以及交叉分类解决方案。

（5）通过连贯一致的举措，保护个人隐私、公民权利与公民自由。

对于保持公众信任来说，提高我们行动的一致性是必不可少的组成部分，依靠我们在整个政府中实施个人隐私、公民权利与公民自由保护，在发展信息共享的过程中建立起相应的保护机制，促进问责机制与遵守规范机制逐渐走向成熟。

在共同执行这一战略的过程中，我们将充分利用集体决议，把信息视为一项国家资产，使它可供所有授权用户发现与检索，并将这些授权用户用信息武装起来，使他们承担保护国家安全的职责。只有我们一起努力，坚持履行自己的职责，协调一致推进我们的目标，我们才能实现国家安全，成功满足我们国家的正当要求，而且这样做是完全值得的。

（一）导言

为了防止在美国本土发生恐怖主义行为，我们必须调动所有情报、执法和国土安全能力。我们将继续整合并利用州和主要城市地区融合中心，它们有能力共享机密信息；建立报告可

疑性活动的全国性体系；对反恐信息系统采用综合方法，确保我们的分析人员、执法人员和官员能够在整个政府范围内获取相关情报。依靠网络连接，我们正在改善信息共享与协作机制，方便联邦、州和地方政府机构部门能够无缝交换消息与信息，执行信息搜索与协作。

——《国家安全战略》，2010 年 5 月

我们的国家安全依赖于我们在合适的时间在适当的人群中共享正确无误信息的能力。由于世界正日益变成一个网络化的场所，解决国家安全面临的挑战——国外的和国内的——需要持续合作并负责地实施信息共享。

保障与保护美国公众的当务之急是各参与部门与机构结成合作关系，包括联邦、州、地方、部落与领地。合作与协同必须发生在情报、防务、外交、国土安全、执法部门以及民营机构之间。

1. 范围

以《2010 年国家安全战略》为支撑，《2012 年信息共享与安全保障国家战略》（以下简称“战略”）为更有效地整合并执行政策、程序、标准和技术，促进安全与负责的国家安全信息共享提供了指导。

《2012 年信息共享与安全保障国家战略》并没有对哪些类型与保密级别的信息必须共享加以限定。相反，它把重点转向信息共享与安全保障政策，这些政策定义了为信息决策提供有效支持的信息需求。这一战略以国家政策路线图的形式勾勒出一种愿景，为在现有法律与政策框架内实施信息共享与安全保障提供了指导意见。这一战略并不会替代《2007 年信息共享国家战略》（2007 NSIS），因为《2007 年信息共享国家战略》将继续提供政策框架，并为改善信息共享指明了许多核心举措。这一战略将继续强调对个人权利的适当保护——在此情况下，个人隐私与公民自由权是最相关的。此外，各部门与机构千万不能忽视自己的责任，要根据各自的职责保护所有美国人的公民权。

2. 愿景

切实有效、适当地共享并保护信息是一个国家的优先事项，这样得到授权的任何个体（联邦、州、地方、部落、领地、民营部门或外国合作伙伴）才能阻止对美国人民的伤害，保护国家安全。

这一战略指明了信息共享未来的发展方向，通过在任何时间向得到授权的任一用户提供正确的信息，信息将为国家安全决策提供支持，而这只能由法律或政策加以约束，技术水平不能成为障碍；在保护措施方面，要包含全面的负责机制，防止信息被滥用。

3. 在成功的基础上开展建设

在 2012 年战略确立未来发展目标的同时，《2007 年信息共享国家战略》继续为《2004 年情报改革与恐怖主义预防法》的制度化要求提供政策框架，特别是改善与恐怖主义、国土安全以及大规模武器扩散相关信息共享的整合与负责情况。《2007 年信息共享国家战略》还凸显了搜集并报告本地生成信息的重要性，同时强调了及时、可直接用于行动的信息在政府、公众以及民营机构间的双向流动。到目前为止，在这些合作伙伴的共同努力下，这些方面的

工作已经取得了显著进步。

建立归州与地方机构所有并管理的全国性网络融合中心，利用全国性可疑活动报告计划（Nationwide Suspicious Activity Reporting Initiative，NSI）在各级政府间共享反恐信息，并采取一贯的政策保护个人隐私、公民权利与公民自由。融合中心、联邦调查局（FBI）联合反恐工作小组、战地与地区情报小组、联邦、州与地方执法机构、高密度贩毒区计划（High Intensity Drug Trafficking Area Programs）、区域信息共享系统中心、情报与犯罪分析单位之间的协作水平已经有了明显提高，并且通过融合联络主任计划等措施，把部落与非执法部门的合作伙伴也包含在内。

接受国家信息交换模型（NIEM），这是一种成功的案例，将常用方式用于结构化数据交换，使信息能够得到更好的共享。目前，国家信息交换模型被许多联邦机构、州政府、民营部门组织和外国合作伙伴使用。

随之而来的另一种好处是，通过与标准制订组织（SDO）合作，国家信息交换模型已经被信息技术产业所接受。

通过《网络空间可信身份标识国家战略》下的联邦身份认证与访问管理（FICAM）框架，确立一项计划，在各个系统上统一并采用一致的用户身份识别与验证程序。这代表着向确立个人负责制并方便信息合理获取方向发展的关键一步。

提供跨机构与部门访问多个数据存储库的通道，与任务职权和法律保护的相关规定保持一致。例如，国家反恐中心（NCTC）的分析人员现在可以访问 30 多套含有恐怖主义分子信息的网络。这与“9・11”事件之前以机构为中心的数据存储仓库形成了鲜明的对比。

国家反恐中心开发了一套单一的权威数据库，存储已知或可疑国际恐怖分子的身份信息。国家反恐中心数据库中的有关信息现在可以导入联邦调查局恐怖分子筛选中心数据库当中，这其中也包括国内众所周知或有理由怀疑是恐怖分子人员的身份信息，相对于以往多套、非集成的列表，这是一个显著的进步。

加强通信，方便各部门和机构与其他合作伙伴开展交流。例如，美国联邦调查局和国土安全部（Department of Homeland Security，DHS），得到跨机构威胁评估与协作小组的支援，全年每天都可以与十几家联邦反恐机构召开 3 次机密视频电话会议。

这些努力产生的成果非常实用，适当时还可通报给非联邦机构的合作伙伴。

通过这些基础工作，我们已经成功开始梳理政策与流程，克服文化上的障碍，改善信息技术系统的互操作性，使相关信息能够得到共享。

（二）作战环境

信息技术的不断进步激励利益相关方确定并实施信息管理的最佳做法。虽然新方法使得信息可以在司法管辖权、功能和组织界限间顺畅流通，不过，信息共享程度得到提高也可能会制造漏洞，使我们受到伤害，影响我们开发、利用信息，并有可能造成未经授权使用信息的现象出现。这些问题经常指向我们在控制、信息管理以及信息来源等方面面临的挑战。

国家安全面临的威胁仍然形式各异。对美国本土及海外利益发动的恐怖袭击，信息系统面对的内部威胁，核扩散，网络攻击，全球经济压力，以及地区的不稳定性是我们面临的不同威胁的一些例子。未来，威胁只会继续演变，因为敌人会研究如何对付我们的安全措施。广泛而动态的一系列挑战表明了我们需要及时而有效地共享信息并加以保护的范围。

管理办法与政策的不相匹配造成障碍。各部门与机构需要认清它们在信息共享与安全保障过程中的法定职责，克服历史上的孤立做法与政策，从整个政府的角度看待问题，并同意参与体系化的协作。更好的协调管理框架为政策与流程的出台提供一种机制，使各参与机构和部门以一种高效且更具成本效益的方式，在信息共享与安全保障过程中各负其责。

共享信息的质量控制是一道难题。为国家安全提供支持的信息可能是不完整的、模糊的或不准确的。开发工具和技术帮助利益相关方在获取、访问、保留、复制、使用、管理、共享和保护信息时评估信息的出处，这对于确保质量控制至关重要。

对存在的共享信息实施有效性约束。对于共享的作战、执法或个人身份信息，做一些限制是必要的。此外，外国合作伙伴、州政府以及民营部门可能会在信息的使用或传播过程中给予一定的限制条件。我们的工作要尊重这种现实，以一种负责任的方式共享信息，如为数据打上“标签”，识别并确认用户身份，保护网络正常工作，这是对此类信息给予适当保护的关键。

网络缺乏互操作性会在各部门和机构与任务间造成障碍。政策与技术上的差异会对授权用户在不同的网络上获取重要资源和信息制造障碍。我们正在努力工作，使互操作性能够满足用户的需要，使他们可以在“敏感但非机密”和机密的网络中访问信息，同时对这些信息保持高级别的保护。

提高信息共享程度需要有先进的关联性与分析能力。把大量数据转化为可据此操作的信息或情报仍然是一个持久的难题。不过，我们正在实施多项计划，使信息能够与先进的分析技术关联起来，这包括开发新的工具，研究新的技术并开展相关培训工作。

讲究效率是必要的。过去几年的经济衰退影响到包括家庭、商业机构与政府中的每一个人。在一个极端苛刻的预算环境中，任务目标必须满足创新与灵活性的要求。

不正确地保护信息是一项障碍。我们正确保护共享信息的能力与控制流程、访问控制、身份管理、企业审核能力以及网络互操作性工作直接相关。这使得我们从在单独的网络与系统中控制质量与访问转向围绕利益相关方对共享信息实施管理。

（三）原则

我国公民的思想、价值观、创新力以及灵活性是美国最重要的资源。我们为预有准备、保持警惕且全力投入的机构的发展提供支持，并且强调我们的公民是国家坚韧不拔的源泉。而且我们必须通过与民营部门、非政府组织、基金会和以社区为基础的机构结成战略合作伙伴关系，有效利用政府之外的创造能力。

这样一种合作关系对于美国在本土与海外取得成功都至关重要，而且我们将通过强化参与、协调、提高透明度与信息共享等机遇对这种关系提供支持。

——《国家安全战略》，2010 年 5 月

为了实现战略愿景，我们的工作要以 3 项核心原则为基础。

1. 把信息视为国家资产

各部门与机构已经具备了史无前例的能力去收集、存储信息，并且在符合它们的任务和

法定职责的条件下使用这些信息。它们有相应的义务使信息可供任何机构、部门或与国家安全任务相关的合作伙伴使用，并且应以一种合法且能够有效保护个人权利的方式管理这些信息。这需要有一种不断走向成熟的信息安全、访问和保护政策与流程。例如，建立一种企业级的方法，把利益相关方从专注于机构本身的网络和应用程序中解脱出来，提供安全且经过授权的信息访问通道，使信息可在各部门与机构间共享。

把信息作为一项国家资产管理的同时，还要求利益相关方将这些信息提供给有需要的人使用，而且要保证它们的安全，不得未经授权或因意外被人利用。虽然信息的原创者要对共享信息的准确性、特征描述和适用性负责，不过，在报告或决策中使用这些信息的用户同样需要对使用它们的方式负责。总而言之，信息的收集、分析并经各利益相关方传播必须是可发现和检索的，要符合必要的法律约束，并由政府各部门的政策、标准以及管理框架加以指引。

2. 信息的共享与安全保障需要各部门与机构共担风险管理机制

在信息的共享与安全保障过程中，各部门与机构建立起彼此之间的信任需要有能力实施管理，而不是规避风险。当信息共享采用一种缺乏一致性、片断式的方法，或从单一机构的角度出发实施管理时，国家安全面临的风险就会增加。不过，采用健全的政策与标准、提高认识、开展较为全面的培训、实施有效控制并强化问责制会降低这种风险。企业层面的绩效管理与合规性监控将为控制、信息决策起辅助作用，并将培养一种文化氛围，强调负责任共享的重要性。

共享与安全保障不是相互排斥的。用于信息共享与安全保障的政策、实践和方法能够在实现适当保密性的同时提升信息的透明度。认识到信息共享的好处，利益相关方采取适当的措施在信息共享过程中建立起彼此之间的信任关系，保护信息免受损害，从而降低风险并对这种风险加以有效管理。由于任务对提高信息共享要求的紧迫性，需要下大力气改善具备互操作能力的安全保障技术。

3. 信息通知决策

知情决策需要能够发现、检索并使用准确、相关、及时、有效的信息。同样，我们国家的安全取决于能否使信息更易于被联邦、州、地方、部落、领地、民营部门以及外国合作伙伴依据适当的任务背景以一种令人信任的方式获取。我们的目标是要通过政策、指导方针、交换标准和通用框架的一致应用，增加作战中的有用信息，同时始终尊重隐私与个人权利。

最终，负责的信息共享的价值将由它对于主动决策的贡献来衡量。上述原则和后文所述目标将帮助我们实现这样一种环境：在该环境中，决策由信息驱动，而且反映我们各级（从前线人员到机构负责人）的最佳评估结果。

（四）目标

1. 通过协作与问责制推动集体行动

（1）改善控制方式，促进合作。

控制在设置优先事项并推动做出决策方面发挥着关键作用。分布在政府各个层面独立承担这些责任的机构，同时也负责性能与合规性监控。应明确它们的工作要求、协调一致，并

且使机构章程具有互补性，为在尽可能低的层次开展合作与执行政策提供支持。此外，通过白宫的决策流程把问题向上级部门提交的方式仍然被允许。一种有效的控制架构会对各种任务的复杂性做出说明，确认来源的真实性，弥补差距，最大限度降低冗余，并且协调利益相关方之间政策的制定与实施。

（2）增加通用流程的使用。

许多机构在采购、获取、保留、生产、使用、管理、共享以及信息安全保障方面采用通用流程。例如，全国性网络融合中心和地方执法机构使用的可疑活动报告流程（包括利益相关方的行为、隐私保护和在全国各地司法管辖区用于确定并报告可疑活动的使能技术）在共享可疑活动报告信息工作方面已被广泛采用。通用流程，如用于可疑活动报告的通用流程，为各机构提供了可重复、具备互操作性以及互信协议的模板。为满足不断发展的任务需求，具备一定灵活性的标准化技术还促进了信息的及时发现、访问与交换，使得将新的合作伙伴纳入现有的信息流当中更为容易。通用流程的利用率升高不仅为加强保护隐私、公民权利与公民自由提供了机遇，而且便于对信息保护措施的审查实施。

（3）理顺信息共享协议的开发。

用于保护国家安全的信息共享依赖于多家政府机构、民营部门和外国合作伙伴所提供信息的有效性，所有这些部门都有不同的任务和不同的信息收集与传播政策。因此，研究制定机构间信息共享的协议往往是跨部门成功合作的关键步骤。遗憾的是，这一步骤经常是旷日持久的，因为参与信息共享的部门试图就信息的获取、处理等方面的事项确定双方都能接受的需求与约束，并根据不同的任务、需求、约束以及权力机构创建的模板使用信息，以共同的法律和政策合规性要求为基础将理顺这一流程，方便问题的解决并强化与民营部门以及与外国伙伴的合作关系。

（4）通过绩效管理、培训与激励机制鼓励发展。

实现这一战略目标需要管理方法，包括在机构与个人层面实施绩效激励。各部门和机构将从整合它们的绩效管理方法中获益，以实现信息共享与安全保障为目标，支持发展的整体观念。

利益相关方不仅要在信息共享与安全保障流程（如可发现性、及时性、准确性、合规性与监督）中对进展情况做出衡量，而且要评估他们的整体效益（如怎样利用共享的信息完成任务）。绩效管理和衡量标准与高效的领导层相结合，会加快工作进度并激励人员满足较高的期望和专业标准。在培训和激励工作人员方面加大投入也有助于促进重视信息共享和行程安全保障文化，这种文化氛围会扩展到我们现有机构之外的组织。

2. 通过通用标准，改善信息的发现与获取

（1）为信息的发现与访问制订明确的政策。

信息共享的核心意图是要使某些信息能够被有合理需求的人员以一种及时的方式发现并访问。发现和访问是两个不同的概念：前者解决用户识别信息存在的能力，后者与用户检索信息的能力有关。我们的国家安全要求相关信息能够按照现行法律与政策被合适的人员发现。发现和访问需要有明确一贯的政策与标准，以及实现互操作流程与工艺的技术指导。

（2）提高标识、身份验证和授权的控制。

信息发现需要有标准化的方法，以便进行身份验证，这样参与机构才能验证并确认试图

登录系统的用户的身份。信息的持有者往往会创建他们各自的认证服务，用户需要不同的凭据访问不同的系统或网络。令人信服、具备互操作性的身份认证服务将最大限度减少所需凭据的数量，去除不必要的匿名，并通过消除独立的认证服务提高效率。

一旦用户身份得到认证，他们独特的属性将帮助确认是否得到授权以访问信息。信息的创建者和用户共担责任，使用标准化的流程、属性以及“使用规则”为身份认证与授权决策提供支持。另外，用户属性需要实施动态管理，明确告知这些决策的出台，包括用于灵活更新和删除用户访问权限的条款。各部门与机构较大的政策与技术调整将实现互操作能力，在确认相应用户的过程中树立起信心和相互之间的信任，同时还会提供访问任务相关信息的途径。

（3）促进数据层标记。

大多数信息授权模型被限制在访问控制领域，在网络或应用程序层加以约束和实施，而不是利用具体信息资源的固有特性在数据层加以约束和实施。随着网络的合并与接受共享服务，访问控制必须将“标签”应用于数据本身。信息标签是一种方法，标准属性——标记——被附加到一条信息上对它加以描述。根据个人资料，指引用户直接访问特定的信息，人工发现与访问能力可从信息标记中获益；信息标签也能根据任务的相关性，自动实施访问决策。

通过把用户属性与相应的信息属性加以匹配，特定任务信息自动化传送的情况得到了改善，同时对信息加密并采取保护措施，使之不能被发送给错误的收件人，在如下几个方面信息标记进一步发挥了辅助作用：满足记录的管理需求，对披露查询做出回应，整合隐私保护，并且对错误的数据披露与更改做出补救。

（4）加强企业范围内的数据关联。

能否把不同部门与机构数据库中的关联信息连接到一起，意味着如下所述的不同结果：一种是在威胁的计划阶段就对它加以确定，而另一种是在威胁已经产生后分析应该采取什么样的措施挫败袭击。数据关联和先进的分析方法，外加一体化的共享与安全保障，将使用户能够参考多个机构拥有的最新的权威信息。这种能力能够为分析人员的工作提供支持，使他们能够确定人员、位置、事件之间的关系，以及其他一些方面并不明显的特征。为了发展这种能力，同时考虑日益增加的数据量，利益相关方需要使他们的信息能够被访问，这样分析人员才能创建一种单一的查询方法搜索大量信息资源。分析人员还需要自动化功能，当存在与任务相关的可用信息时，在拥有信息和发出警报之间建立联系，虽然目前的技术需要集中式的数据仓库，它在有限的条件下还可能适当保留，不过，分布式处理的办法使创建者可以根据需要维护并更新信息。这能够提高信息共享的速度，并使信息的保真度更高。成功的数据关联同样需要有一套验证组件在行动之前确定信息的准确性和适用性。

（5）推动采用信息共享标准。

满足任务需要，在企业范围内查找授权使用信息的标准。采用其他手段需要全面审查并实施新的标准，而依靠重新利用已有标准，利益相关方可从以前投入的时间、资源和经验中获益。这样做可以更加迅速、切实有效地满足需求，因此不必研究专门的定制解决方案或仅为一次应用制定专门的标准。参与信息共享且富有远见的部门与机构利用自愿达成的共识，确定了标准做法（正如现有联邦政策中描述的那样），其中政府采用标准化组织已经确立的标准，这些标准化组织往往包含了政府、产业界以及国际会员。

依靠这种方法，我们的目标是先采用现有标准满足任务需要，当没有适用标准时，利用

标准制定组织弥补这种不足。

（6）支持企业范围内的认证与一致性。

由于缺乏适用于整个政府、民营部门以及国际机构的标准，决策者与用户面临着挑战，即确定哪些标准最能满足用户需求，同时还满足与其他伙伴的互操作性要求。因此，有必要利用一个流程对要采用的标准加以验证、确认，并要求技术解决方案的互操作性可用于共享和保护信息。这还会告知决策者采用哪些最为合适的标准，同时向业界发出信号，可以使用哪些标准开发工具和产品推进互操作性的发展，并为更广泛的任务需要提供支持。

3. 通过共享服务与互操作性优化任务效能

（1）共享服务有利于所有合作伙伴。

在整个政府范围内，各部门与机构已经开始接受共享的计算模型，也称“云计算”。在该模型中，数据中心被合并，计算机基础设施被当做一种共享服务加以应用。由共同基础设施上的主机系统和应用程序分配工作量，这降低了对于计算能力的要求并削减了总成本。通过提供共享计算之外的能力，如共享应用程序和共享信息服务，未来有望引进额外的增强功能。因此，各部门与机构可以接受现有的能力，专注于开发最符合自身任务和专业的服务与技术。特别是共享功能将使各部门与机构能够更好地把目标服务传送给特定终端用户，而不是试图服务于所有类型的用户，提供所需的全部功能。这种方法的优势包括精简成本，提高效能，并且有可能减少独特接口和所需标准的数量。

（2）改善确定的数据、服务和网络互操作性。

虽然共享服务模型提供了显著的增强功能，但它并不能保证互操作性或信息共享的情况得到改善。各部门与机构继续设法解决由于使用旧的数据、服务与系统带来的问题，那些过时的技术已经不同程度地与各种机密和非机密的网络连接在一起。信息技术的发展往往没有对互操作性问题给予足够的重视。依靠在信息技术解决方案的设计阶段进行规划并给予优先考虑，各部门与机构能够享受到跨机构实施互操作性所带来的优势，同时满足个别任务的授权需要。提高互操作性并得到共享的服务与信息将提高任务的成功率，最大限度地降低复杂度，并减少重复，降低当前的维护要求。

（3）通过采购支持集体需求。

对于部署具备互操作功能的技术解决方案和共享服务来说，结合标准的采购方式十分必要。当政府部门和机构或与产业界结成合作伙伴关系，确定并重复使用政府已经处理过的最好解决方案，并且开发基于标准的技术，为多项任务和多家机构提供支持时，我们用于系统集成和信息共享的能力将得到进一步的增强，并且更具灵活性。利益相关方得到鼓励，与产业界共同合作，开发、采购利用信息共享与安全保障标准的工具与技术。联邦采购政策，包括无偿援助政策，将促进部门与机构间的合作，并对它们给予奖励，这会促进重新利用现有服务，并鼓励企业层采购的重点发展。调整采购要求不仅要支持互操作技术的需要，而且要依靠更小的采购规模和降低处理成本，尽可能缩减各部门与机构增加的成本。

4. 通过结构改革、政策和技术解决方案强化信息的安全保障

（1）改革结构与政策。

最近发生的信息泄露与披露事件凸显了在保护敏感与机密信息方面存在的漏洞。不过，继续实施结构改革并推行标准化政策将加强监督工作，向安全方面的最佳做法看齐。未经授

权披露和滥用信息的风险源于内部威胁和外部入侵，结构改革必须解决这两个问题。对信息进行安全保障的能力取决于政策和程序的实施与加强，使网络能够监控、侦测异常行为，确定内部威胁和外部入侵。现有协调机构对于信息安全保障高度关注，同时有责任制定有效的技术政策与标准，协调政府各部门实施；执行独立的合规性评估，并拥有高级官方职责。准实时的跨多个网络与领域的反间谍、保密、信息安全保障以及人力资源要素，使合适的机构能够积极主动地减少并处理安全漏洞。同样，发展协调一致的体系能力，监控网络的健康状况并检测恶意访问企图，需要全面了解应用程序和服务是如何跨网络、跨保密级别应用的。制定的政策与程序还应该解决信息意外泄露的问题。预防、监控和减轻风险的政策，与适当的支持性政策相搭配，可以帮助建立伙伴之间的保证与信任关系，放心地共享信息。

（2）加强数据层控制、自动化监控与跨保密级别解决方案。

在我们发展安全保障能力的过程中，技术同样发挥着重要作用。不断进步需要我们采用具备互操作能力的应用程序把工作重点从网络转向数据层控制。无论信息在什么样的环境下流动，安全控制的粒度越细，越能改善对于信息的访问状况，并加强对于信息的保护，防止信息在未经授权的情况下被披露、传播、访问和修改。自动化的持续监控，配合适当的隐私保护措施，将为共担风险的管理模式提供支持，并能够准实时地描绘现有风险或新出现的风险。过去，信息安全保障工作的重点主要限定在特定保密级别的系统与网络上。不过，各部门和机构往往一致认为需要跨系统安全地共享信息，无论这些系统处于什么样的保密级别。技术、功能和服务（诸如共享计算），进一步促进了对于跨保密级别实施共享的需求。因此，我们需要制定技术、标准和通用流程为这种重要的新兴需求提供支持。

5. 通过一致性与合规性保护隐私、公民权利与公民自由

（1）提高政府各部门保护应用的一致性。

保护个人隐私、公民权利和公民自由是维持公众信任不可分割的一部分，这是我们信息共享与安全保障工作的基石。各部门与机构需要采取一致的方法保护它们控制的基本隐私、公民权利与公民自由，并根据现有法律和政策提供适当的任务灵活性。利用管理机构和现有程序，不断完善并建立必要的指导方针，对共享信息提供适当保护，如《信息共享环境隐私保护准则》（Information Sharing Environment Privacy Guidelines）。培养一种全面而有效的方法，在联邦与非联邦合作伙伴信息共享过程中定义并实施个人隐私、公民权利与公民自由保护，维持适用的法律、法规与政策要求。当务之急是既要保证国家安全，又要保护个人隐私。

（2）在信息共享行动发展过程中建立保护机制。

保护个人隐私、公民权利与公民自由不是法律顾问和专门问题专家的专属领域。控制信息使用和保护以立法与政策制定方式实现，并与技术实现相融合。这值得项目经理、系统架构师与开发人员、信息安全保障人员以及项目与系统设计中的其他人员参与、协调。在任何新举措的初期阶段（或者在现有系统与流程的重新设计阶段）解决个人隐私、公民权利与公民自由等问题，使这些信息的保护措施可以在整个企业范围内加以考虑、整合、管理与监控。

（3）促进问责制与遵守法规机制。

通过监督、绩效管理确保遵规守法。另外，在问责制中适用采用执法机制与确定采取保护措施同等重要。当前，各部门与机构就其在个人隐私、公民权利与公民自由保护等方面的严谨性实施监督并做出报告，在此过程中，这些机构与部门采用了适当的合规性文档与绩效

管理技术。问责制中采用的监控与衡量合规性验证机制在确定和处理漏洞方面对任务伙伴起辅助作用，同样的作用还体现在验证他们是否主动并系统化地完善对于个人权利的保护方面。在向企业方法过渡过程中，必须不断强化保护措施并实施评估，包括监控访问与应用控制、审计和用途信息的分析，开展定期、系统性的合规性审查。

履行保护个人隐私、公民权利与公民自由的相关义务，符合相关规定，必须随着信息共享需求与技术的变化向前发展。展望未来，这种企业范围模型将包括利用政策，评估和强化个人隐私、公民权利与公民自由保护要求。

（五）未来发展方向

正如《美国国家安全战略》中所阐述的那样，“各政府部门开展合作，并与各州、地方和部落的伙伴以及产业界和国外的合作伙伴开展合作，必将为我们的活动提供指导。”

该战略作为一个指南，用于平衡各方工作，促进信息共享与安全保障工作，为国家安全提供支持，提高美国人民的安全水平。总之，我们可以超越传统意上的信息共享协议，深入我们的使命，当得到所有相关信息的支持时，指导有关机构与部门做出自信的决策，使民众得以更好地了解。不过，这同样需要有一种平衡投入，对信息本身、信息来源以及收集方法实施适当的安全保障，同时还需要尊重相关法律与政策的规定。我们的事业取得成功取决于共同努力，在信息共享与安全保障之间实现平衡，它建立在以往成功的基础之上，并依赖于不断成熟的信息共享环境。

应该制订综合实施计划，为实现这一目标提供协调和可持续发展的方法，并对这一战略的远景有清醒的认识。这一计划将侧重于实现优先目标，以 5 年期限对利益相关方的行动进行排序，包括绩效管理与里程碑，并指定牵头部门与机构。这一实施计划将把年度计划与实施指导原则加以整合，与联邦预算周期保持同步，并保持适当的灵活性，可以对活动加以调整，根据年度绩效管理、重点更替和资源分配予以交付。计划在实施过程中将包括为国家安全提供支持的所有部门与机构，这些部门与机构由白宫领导，该实施计划利用管理与预算办公室的战略资源分配流程，在适当条件下，根据任务相关性与现有权限，由各部、局和行政机构管理。

优先目标具体如下。

1. 五大目标

以下是政府当局在实现信息共享与安全保障战略目标过程中总结出来的五大优先事项。

（1）理顺信息共享与安全保障的管理，促进更好的决策、绩效、负责制以及战略目标的实施。

（2）为信息共享与安全保障协定制订指导原则，解决共同的需求，包括个人隐私、公民权利与公民自由的保护，同时允许在满足任务需求的过程中采取一定的灵活性。

（3）采取元数据标准，以便在联邦网络和安全领域中促进数据的联合发现、访问、关联与监控。

（4）把联邦身份认证与访问管理路线图扩展到整个安全领域并加以实施。

（5）采取可移动的媒介政策、流程与控制；对资产、漏洞和威胁提供及时的审查能力；确立程序、流程与技术，制止、检测并消灭内部威胁；共担风险管理，加强非机密与机密信

息的安全保障工作。

2. 其他优先目标

其余目标代表着各部门、机构和利益相关方为推动这一战略目标的实现应实施的另外一些优先活动。

（1）定义并接受基本能力和通用要求，使数据、服务和网络具备互操作性。

（2）使用共同、量身定制的课程为合适的利益相关方提供信息共享、安全保障和处理培训，促使它们形成一致、灵活且值得信赖的流程。

（3）制定并实施共同的流程与标准，为基于策略自动化发现与访问的决策提供支持。

（4）确立信息共享流程，以及各部门与民营部门合作伙伴的具体协议，提高信息的质量和及时性并保卫国家的基础设施。

（5）制定参考架构，为在不同的数据集中采用一致的方法实现数据发现与关联提供支持。

（6）在合适的利益相关方中执行《联邦信息共享服务战略》所提出的建议与活动，促进其接受共享服务。

（7）细化标准认证和一致性流程，在部门与机构、标准化组织和供应商之间实现基于标准的采购，促进产品与服务的互操作性。

（8）促进各方遵守现有跨部门流程，与外国合作伙伴协调信息共享计划，接受并实施必要的指导方针，遵守法定机构与总统政策的要求，确保在信息共享与安全保障中保持一致。

（9）在各级政府中创建信息请求、警报、提醒与通知的通用流程，使它们能够及时接收并传播信息，并且做出适当反应。

（10）完成全国性可疑活动报告计划（NSI）在全国网络融合中心和联邦机构内的实施，同时扩大培训与宣传范围，除执法部门外还要包括公共安全机构。

（11）实现 4 种关键的作战能力、4 种使能能力及其他优先目标，在州与地方环境内围绕全国网络融合中心，使之能够有效并合法地发挥作为一个重点的作用，用于接收、分析、搜集并共享与威胁有关的信息。

整个政府内的国家安全利益相关方，以我们共同的原则为指导，现在可以采取一致的行动来实现这些优先目标，确定执行计划以实现这一战略目标。

随着我们合力执行这一战略，我们将充分利用集体决定，把信息作为一项国家资产，使它能够被所有授权用户发现和检索，用所有可用信息对那些负责维护我们国家安全的机构进行武装，推动它们做出正确的决策，保护我们的国家和人民。只有我们齐心协力，把握自己的责任，发挥与我们实现目标相一致的作用，才能成功实现我国的合理要求，这是完全值得的。

国防部网络战略

一、引言

我们生活在一个网络互连的世界。从公司财务交易，到国家的军事力量运作，全都依赖着网络空间。计算机代码使网络与现实世界之间的界限变得模糊起来，并在互联网或专用网络上将数以百万计的对象联系到一起。电力公司依赖于工业控制系统为电网提供电力。船务经理使用卫星和互联网相结合的方式，在通过全球的航海线时跟踪货轮。美国军方依赖于安全网络和数据，履行其使命。

美国致力于打造一个开放、安全、互操作和可靠的互联网，促进繁荣、公共安全和贸易及思想的自由流动。互联网的这些特点反映了美国的核心价值观——言论自由和隐私、创造力、机会和创新。这些特点使互联网向数十亿人民提供了社会和经济价值。单单是美国经济，各地方 3%～13%的增值来源于互联网相关业务。在过去十年中，全球各地的互联网访问人数增加了 20 多亿。然而，同样是这些开放和活力的特点，使互联网快速扩张，现在却为危害国家和非国家行为者破坏美国的利益提供了一种手段。

在这个网络互连的世界中，我们都是脆弱的。今天，我们对数据的保密性、可用性和完整性的依赖，与我们的网络安全不足形成了鲜明的对比。最初互联网的设计不是为了安全，而是作为一个开放系统，使科学家和研究人员能够快速将数据发送给另一个人。由于没有在网络安全和网络防御方面加强投资，数据系统保持着开放的状态，并容易受到基本和危险形式的利用和攻击。恶意行为者为了他们自己的经济或政治目的，使用网络空间来窃取数据和知识产权。在世界某个地方的行为者可能使用其网络能力，直接在数千英里之遥的地方破坏网络，破坏数据、扰乱业务，或关闭关键系统。

国家和非国家行为者进行网络行动，以达到各种政治、经济和军事目的。在进行其业务时，他们可能侵袭一个国家的价值观、利益或目的。例如，2014 年 11 月，似乎是为了报复预计发布的讽刺电影，朝鲜进行了针对索尼影视娱乐公司的网络攻击，使索尼成千上万台计算机无法操作，并破坏了索尼的机密商业信息。除了攻击的毁灭性特点，朝鲜还偷走了大量未发行的电影，以及数以千计的文件，包含有关名人、索尼员工和索尼公司业务运营的敏感数据。在进行网络攻击的同时，朝鲜还进行了胁迫、恐吓和恐怖主义式的威胁。朝鲜对索尼的攻击是到目前为止针对美国实体最具破坏性的网络攻击之一。这次攻击进一步刺激了已经正在进行中的全国关于网络威胁和需要改进网络安全的讨论。

使用网络攻击作为一项政治工具的增加，反映了国际关系中的危险趋势。易受侵害的数据系统为国家和非国家行为者袭击美国及其利益提供了诱人的机会。

在冲突期间，国防部假定一个潜在的对手将寻求对付美国或其盟国的重要基础设施和军事网络，以获得战略优势。超出上文所述的攻击，一个老练的行动者能够针对公用事业的工业控制系统（ICS），来影响公众的安全，或进入一个网络，以操纵健康记录来影响个人的健康。如果失去生命，毁坏财产，政策目标受到破坏或经济利益受到影响，一次破坏性、操纵

性或毁灭性的网络攻击可能给美国经济和国家安全带来重大风险。

领导人必须采取措施来降低网络风险。各国政府、公司和组织必须仔细确定需要优先保护的系统和数据，评估风险和危害，并在网络安全和网络防御能力方面做出审慎的投资，以实现其安全目标和目的。在这些防御投资的背后，每一种组织必须建立业务连续性方案，准备在退化的网络环境中运行，在这个环境中，网络和数据访问存在不稳定性。并且如果必要的话，为了减轻网络空间中的风险，需要一项全面战略对抗和抵御破坏性和毁灭性攻击。

（一）防御网络空间中的美国

美国国防部（DOD）与其他机构一道，负责保卫美国本土和美国的利益免受攻击，包括可能发生在网络空间中的攻击。采用符合美国法律和国际法律的方式，国防部旨在遏制攻击和捍卫美国，反对任何意图在和平、危机或冲突时期危害美国国家利益的敌人。为此，国防部发展网络运行的能力，将这些能力集成到全方位工具组中，美国政府用此来捍卫美国的国家利益，包括外交、信息、军事、经济、金融和执法工具。

在过去 4 年中，2011 年 5 月发布的国防部《网络空间行动战略》指导国防部的网络活动和支持美国的国家利益行动。这个新的战略为国防部的网络活动和任务设定了要在未来 5 年内优先实现的战略目标。它致力于建设有效实现网络安全和网络行动的能力，来保卫美国国防部网络、系统和信息；帮助国家抵御网络攻击；支持行动和应急计划。这一战略是建立在之前关于发展国防部网络特派部队和网络劳动力的决定之上的，它提供全新和具体的指导，以减轻预期的风险，抓住机遇，加强美国的国家安全。

作为第一项原则，网络安全是美国联邦政府内部团队的努力。要在其任务上取得成功，国防部必须与其他部门和机构、国际盟友和伙伴、国家和地方政府形成合作伙伴关系，最重要的是要和民营部门合作。

（二）安全行动

为了支持其网络空间的特派部队，国防部在网络空间以外的地方进行了一系列的活动，以提高集体网络安全及保护美国利益。例如，国防部与美国政府机构、民营部门合作，与国际伙伴分享信息、建立联盟和伙伴关系，并提高负责行为规范，来加强全球战略稳定。

（1）信息共享和部门协作。为了保护和推进美国在网络空间中的利益，国防部在一系列的网络活动中以综合的方式，与美国政府部门分享信息并协作。例如，如果国防部获悉恶意网络活动会影响美国重要网络和系统，对美国国家和经济安全或公共安全至关重要，国防部会在探寻美国实体的时候，支持国土安全部（DHS）和联邦调查局（FBI）等机构，并经常与其他国家分享潜在攻击的技术指标等威胁信息。这种信息共享，可以显著提高一个组织的能力，以抵御种类繁多的网络攻击。除了分享信息，国防部与美国政府其他部门合作，同步操作并分享经验教训和网络安全的最佳做法。这包括事件管理和网络防御反应。

（2）为民营企业建立沟通桥梁。从应用程序开发人员到互联网服务提供商，私人公司为网络空间提供了商品和服务。国防部依靠民营企业建设其网络，提供网络安全服务，并研究和开发高级功能。在其整个历史中，国防部已经受益于民营企业的创新。展望未来，国防部将与民营企业密切合作，以验证和商业化部门网络安全的新思路。

（3）建立联盟、同盟和国外伙伴关系。国防部从事各种各样的活动，以提高国外网络安

全和网络操作能力。国防部帮助美国的盟友和伙伴了解它们所面临的网络威胁，建立保卫其网络和数据的必要网络能力。盟友和伙伴通常也有互补功能，可以增强美国的能力，美国试图建立强大的联盟和同盟对抗潜在的网络活动对手。在战略上，一个统一的同盟发送一条信息，美国及其盟友和伙伴集结起来集体防御。除了五只眼条约伙伴，国防部密切配合在中东地区、亚太地区和欧洲的重要合作伙伴，了解网络安全环境，并建立网络防御能力。

（三）网络安全的三大主要任务

总统已设立管理网络行动的原则和过程。这些原则和过程的目的是计划、开发和有效地利用美国的能力，并确保网络行动以符合美国在国内和国际上推行价值观的方式进行。

国防部有三个主要的网络任务。

第一，国防部必须保护自己的网络、系统和信息。美国军方的运行依赖于网络，2011年美国国防部部长宣布将网络空间作为一个业务领域，其目的是组织、培训和装备美国军队力量。国防部必须能够保护自己免受网络攻击，并且如果安全措施失效，能够快速恢复。为此，国防部在现行的基础上不断地进行网络安全操作，以安全运行国防部信息网（DODIN）。当国防部检测到其网络内的敌对活动迹象时，国防部有快速反应能力，关闭或降低其脆弱性，保护其网络和系统。国防部的网络防御操作占据了国防部在网络空间操作的绝大部分。

除了国防投资，国防部必须准备好在一个争议如何访问网络空间的环境中运作。在冷战期间，部队要准备在访问通信可能被对手的高级能力中断的环境中运作，包括电磁脉冲的潜在使用，可能会破坏卫星和其他全球通信功能。指挥官进行定期演习，需要他们的团队在不访问通信系统的情况下开展活动。通过多年的实践和锻炼，抗灾意识已扎根在部队中，并且各部门准备好在竞争激烈的环境中工作。

冷战结束以来，年轻的一代已经越来越习惯于一个有互联网的环境。自冷战结束以来长大的男女军人，经常接触信息和通信，并且信息革命导致了敏捷力和全局自适应力的提升。面对不断升级的网络威胁，现在必须将前几代人的经验教训传递下去。国防部必须履行职责，以保卫国家。组织必须学会在没有工具的情况下操作，这些工具已成为它们日常生活和行动中的重要部分。

第二，国防部必须准备保卫美国及其利益，抵御有严重后果的网络攻击。网络攻击由总统和美国的国家安全团队在个别情况及具体事实的基础上进行评估，重大的后果可能包括生命损失、重大财产损失、对美国外交政策造成严重不良后果或对美国经济造成重大影响。

如果由总统或国防部部长领导，美军可能会采取网络行动，对付迫在眉睫或正在进行的袭击美国本土或损害美国在网络空间利益的行为。这种防御性措施的目的是减弱攻击并防止破坏财产或生命损失。国防部试图与其他政府机构职能同步，开发了一系列的可选措施和方法，在造成重大后果的网络攻击产生影响力之前，实施干扰，包括执法、情报和外交工具。作为一项原则，在进行网络空间行动之前，美国将设法用尽所有的网络防御和执法选项，降低任何针对美国本土或美国利益的潜在网络风险。

美国政府在保卫国家、抵御有重大后果的网络攻击方面，可以发挥其有限和特殊的作用。民营部门拥有和经营超过90%的网络和基础设施，因而它们是第一道防线。改善美国整体网络安全态势最重要的步骤之一是，公司优化它们必须保护的网络和数据，并投资于改善它们自己的网络安全。美国政府必须准备帮助国家抵御最危险的攻击，公司可以而且必须通过相

对基本的网络安全投资来终止入侵的主体。

第三，如果由总统或国防部部长领导，国防部必须能够在网络上发挥作用，支持军事行动和应急计划。总统或国防部部长恰当的决定，是让美国军方进行网络操作，扰乱对手军事相关的网络或基础设施，以便让美国军队在一个运作领域内保护美国的利益。例如，美国军方可能在美方的立场上，使用网络行动终止持续不断的冲突，或扰乱对手的军事系统，防止其使用武力损害美国的利益。美国网络司令部（USCYBERCOM）也可能受命进行网络操作，在适当的时候与其他美国政府机构一道阻止或打败其他领域中的战略威胁。

为确保互联网保持开放、安全和繁荣，美国将坚持在原则的限制下进行网络行动，根据需要保护人类生命，防止财产破坏。对于其他的业务领域，在网络空间中国防部的行动将会一直体现不朽的美国价值观，包括支持法治，以及尊重和保护言论自由和隐私、信息、贸易和思想自由传播。在国防部网络之外进行网络行动，一切决定都要经过周全的考虑和审议、严格的政策和运作监督，并符合武装冲突法律。在投资和建立网络能力，维护美国国家利益的同时，国防部会一直关注国防政策对国家和非国家行为者的行为的潜在影响。

（四）一支全新的网络任务力量

国防部需要多方领导人和社区的承诺和协调，国防部与美国政府其他部门一道履行使命并执行这一战略。国防部在执法、情报、反谍报和政策组织等方面都具有积极作用。每个组织都要发挥其作用。例如，国防部的网络服务提供商必须自我适应，积极遵循网络安全的最佳做法和网络防御命令。美国网络司令部必须与国防部的其他组织同步行动，尤其是战斗命令，对出现的挑战和机会做出反应。网络设施所有者和经营者必须与军事部计算机应急反应小组（CERT）、国土安全部（DHS）和 USCYBERCOM 合作，为任务关键型系统建立自适应的防御和连续性计划，并建立支持它们的民事制度。成功需要创造性和较强的部门内及跨部门伙伴关系。

在美国国防部的网络人员和部队中，网络特派部队（CMF）具有独特的作用。2012 年，美国国防部开始建设 CMF 执行国防部的网络任务。一旦全面运作，CMF 将跨越军事部门和防御部门，包括近 6200 名军事人员、文职人员和承包商支持人员。在整体上，网络特派部队代表着国防部和美国的重大投资，这一战略的一个中心目标是要确定具体的目标和目的，以指导网络特派部队的发展和国防部更广泛的网络劳动力量，保护和防卫美国国家利益。

网络特派部队由网络运营商组织，形成 133 支团队，主要有以下合作：网络保护部队将增加传统的防御措施，并捍卫国防部一级网络和系统，对抗首要威胁；国家特派部队和其相应的支持团队将捍卫美国及其利益，抵御有严重后果的网络攻击；打击特派部队及其相关支持团队将通过产生综合网络空间影响，支持战斗指令，支持业务计划和应急行动。战斗命令将打击特派部队和网络保护小组纳入计划和行动，在网络空间雇用它们，而国家特派部队在 USCYBERCOM 的指挥官领导下运作。此外，团队也可以根据部门需要，支撑其他团队。

2013 年，国防部开始将 CMF 纳入更大的多任务美国军事力量来实现跨域协同作用，确保 CMF 在军事范围内准备妥当，并重组军事及文职工作人员队伍和基础设施，执行国防部的任务。

在实施这一战略的过程中，国防部将继续建设 CMF，继续完善必要的指令、控制并允许组织所需的切实有效的行动。国防部将工作重点放在保证部队群联，演练各机构需要的网

络智能和体系结构，继续建立政策和法律框架来规范 CMF 人员雇用，将 CMF 纳入国防部的总体规划和部队建设之中。

这一战略认识到，有效的网络安全需要国防部内部和整个联邦政府、行业与国际盟友和伙伴的密切合作。鉴于领域内利益攸关方数量之多、种类之繁，跨越国际边界的信息流动，以及分布于政府和民营企业间的职责、权利和能力，在网络空间寻求安全需要政府全体和国际途径。对于每个国防部的特别团队，国防部必须继续发展常规关系和协调其网络业务流程。

具体的风险和机会贯穿于这项新战略。例如，国防部自身的网络是由分布在世界各地、各式各样数以千计的网络共同构成的，并且国防部还不具备可见的能有效保卫其冗杂的网络所需的组织结构。国防部必须进一步发展充分的预警情报，探知对手意图，提高对抗针对国防部和美国的破坏性和毁灭性网络攻击的能力。除了自身的网络，国防部的运作依赖于美国各地及海外的重要民用基础设施，然而这种关键基础设施的网络安全存在不确定性。

为了降低这些已知风险和其他风险，提高美国的国家安全，本战略为国防部设置了要实现的战略目标，并规定了具体目标和指标。这一战略的所有目标和任务反映了 2015 年美国国家安全战略和 2014 年四年防务评估报告的目标。

国防部为其网络空间任务设定了 5 个战略目标。

（1）建立并维护预备力量和能力，实行网络空间运作。

（2）保卫国防部信息网络，保护国防部数据，规避国防部任务风险。

（3）准备保卫美国国土和美国重要利益不受有重大后果的破坏性或毁灭性网络攻击。

（4）建立并维护网络可选项，规划使用这些选项能够在各阶段控制冲突升级，打造有利的冲突环境。

（5）建立并维护强大的国际联盟和合作关系，阻止共同威胁，加强国际安全和稳定。

二、战略背景

（一）重大网络威胁

从 2013 年到 2015 年，国家情报主管将网络威胁列为美国的头号战略威胁，这是自“9 •11”事件以来，首次将其排在恐怖主义前面。潜在的国家和非国家对手进行恶意的网络活动，在全球损害美国利益，意图测试美国和国际社会的容忍度。行动者可能会以各种目的渗透美国网络和系统，如窃取知识产权，因激进目的而扰乱社会组织运行，或进行破坏性和毁灭性的攻击，以达到军事目的。

潜在对手在网络中已有大量投资，针对美国本土，损害美国利益。俄罗斯和中国已发展了高级网络能力和战略。俄罗斯行动者隐身在他们的网络谍报中，他们的意图有时很难辨别。伊朗和朝鲜有较发达的网络能力，针对网络空间中的美国和美国利益，它们已经显示出了明显的敌对意图。

除了基于国家的威胁外，非国家行为者使用互联网络，招募战斗人员并开展宣传。犯罪人员在网络空间构成巨大威胁，尤其是针对金融机构和智库，经常使用黑客手段以实现自己的政治目标。国家和非国家威胁也经常混到一起；爱国实体经常作为国家和非国家实体的网络代理，还能为国家运营商提供掩护。这种做法会使溯源更加困难，增加了误判的可能性。

（二）恶意软件激增

恶意代码或软件的全球扩散会增加美国网络和数据的风险。为了实施具有破坏性或毁灭性的网络操作，针对军事系统或工业控制系统运行，需要专门知识，但潜在的对手不需要花费数十亿美元来开发一种新的进攻手段。民族主义国家、非国家团体或个别行为者可以在黑市上购买具有破坏性的恶意软件和其他工具。国家和非国家行为者也会雇佣网络专家去寻找漏洞并开发利用。这种做法开辟了一个危险和不受控制的市场，在国际系统内用于多个行为者，其行为的目的是经常相互竞争。随着时间的推移，网络攻击能力变得更容易获得，国防部门将评估国家和非国家行为者旨在针对美国利益寻求和发展网络攻击能力的情况。

（三）国防部网络和基础建设风险

国防部自身的网络和系统很容易受到入侵和攻击。除了国防部自身的网络，国防部赖以运作的重要基础设施和资源也容易遭受网络攻击，甚至会影响美国军方在意外事件中的运转能力。以专门预案的形式，美国国防部已经在确认自身重要资产的网络漏洞方面取得成效，国防部已将许多重要资产确定为重要有形资产所依赖的有形网络基础设施并加以更加严格的保护。

除了破坏性和毁灭性的攻击之外，网络攻击者还会从美国政府和影响国防部门的商业实体，窃取业务信息和知识产权。受害者包括武器开发人员，以及通过美国运输命令（USTRANSCOM）支撑国防装备的商业公司。某些国家已经窃取了美国国防部的知识产权，削弱了美国的战略和技术优势，使它们自身军事和经济发展受益。

最后，国防部还面临着来自美国政府预算持续不确定的风险。虽然美国国防部在其发展网络能力的预算中已经优化了资源配置，但是持续的财政不确定性需要国防部在不断降低整体国防预算的条件下，规划建设其网络攻防能力。美国国防部必须继续优先考虑其网络投资和发展捍卫美国国内外利益的能力。

（四）未来安全环境中的威慑

面对不断升级的威胁，国防部必须促进全面网络威慑战略的发展和实施，以防止重要的国家和非国家行为者攻击美国的利益。鉴于在网络空间中国家和非国家网络行为者的种类和数量，以及破坏性网络工具的相对可用性，一项有效的威慑战略需要一系列的政策和手段，确保足以影响一个国家或非国家行为者的行为。

美国国防部认为，在建立网络特种部队和提升整体能力的同时，仅仅通过发布网络政策，对以美国利益为目标的网络攻击进行威慑不会收到成效，需要借助美国各部门整体的行动，包括宣示政策、实质性的通告和预警能力、防御姿态，制定有效的反应流程并增强美国网络及系统的整体弹性。对网络空间中的国家和非国家团体的威慑将需要多个美国政府部门和机构通力合作。国防部在其中扮演着特殊的角色。

美国必须声明或显示有效的反应能力，以阻止对手发起的攻击；建立有效的防御能力，降低潜在攻击的成功率；加强美国系统的整体适应能力，抵御能渗透到美国防御系统的潜在攻击。此外，美国需要强大的情报、取证和指示及预警能力，以减少在网络空间中的匿名现象，增强信息源的保密性。

- 反应：美国已明确立场，将通过自身的防御能力，回应针对美国利益的网络攻击。在递交 2011 年国会的国防部网络空间政策报告《2011 年美国网络空间国际战略》中，以及总统和国防部部长的公开声明中，美国政府已经阐明了其政策。美国将继续回应每次针对美国利益的网络攻击，并在合法的前提下在美国选择的地点运用适当的手段。
- 反制：虽然美国国防部在建设网络特遣部队方面取得了进展，但美国国防部必须增强其防御能力，以保卫国防部网络和国家不受到复杂的网络攻击，必须与其他部门、机构、国际盟友和合作伙伴，以及民营企业一道工作，加强威慑力量。
- 恢复能力：国防部现有的能力不能保证每次都能成功挫败网络攻击，国防部有必要投资于恢复能力和冗余系统，以便在面对针对国防部网络的破坏性或毁灭性网络攻击时，能够继续开展业务。当然，这种恢复能力必须在国防部的领导下。为了使恢复能力成为一种有效的威慑力量，政府的其他机构必须与重要基础设施所有者和经营者以及民营企业开展更广泛的合作，建立恢复及冗余系统，以抵御潜在的攻击。有效的恢复措施有助于让潜在的敌人认识到对美国的网络和系统进行网络攻击是枉费心机。

信息源是有效的网络威慑战略的一个基本部分，匿名制使国家和非国家团体有机会进行恶意网络活动。关于情报、信息源和警告事项，美国国防部和情报部门已经投入了大量资金在所有来源收集、分析和传播手段上，所有这些都有效减少了在网络空间中国家和非国家行为者的匿名行为。情报和信息源手段有助于最终确定行为者的网络角色、识别攻击的源点，以及确定战术、技术和程序。信息源使国防部或其他机构可以针对来自外部的网络攻击，进行回应与反制。

首先，公共和民用的信息源可以在阻止网络行为者进行攻击方面发挥重要作用。国防部将继续与民营企业和美国政府的其他机构密切合作，加强信息源。随着时间的推移，极端组织、犯罪组织和其他行动者有条件获取先进的网络工具，这项工作对于威慑他们特别重要。

其次，网络攻击能力为国家和非国家行为者提供了打击美国利益的能力，有可能引发美国的军事反应，但这足以对美国国家安全产生重大威胁，引发某种非军事反应。为了回应攻击和入侵，美国可能采取外交行动和执法行动，并考虑经济制裁。

三、战略目标

为了在当前和未来的安全环境中降低风险和捍卫美国的利益，国防部概述了五项战略目标，并为其活动和任务规划了具体目标。

（一）战略目标一：建立并维护预备力量和能力，实施网络空间运作

为了在网络空间中有效运作，国防部要求部队和人员都接受最高标准的训练，准备好并配有同等最佳的技术能力。2013 年，国防部创立了 CMF，在网络人员和技术方面启动了重大投资；现在国防部必须用好这项投资，培训人员，建立有效的组织和指挥控制系统，充分发展国防部在网络空间中运作所需的能力。这一策略为国防部在未来五年及以后满足其部署、培训并且装备部队及其人员设置了具体目标。

（二）战略目标二：保卫国防部信息网络，保护国防部数据，规避国防部任务风险

虽然美国国防部无法避免每个网络和系统受到入侵——国防部的整体网络攻击面太大以至于无法抵御所有的威胁，又因过于庞大而无法关闭所有漏洞——但国防部必须采取措施确定、优化并捍卫其最重要的网络和数据，以便有效运行。如果针对美国国防部网络和数据的攻击成功，或者国防部所依赖的用于运行和应变计划的重要基础设施部分被扰乱了，国防部还必须计划和实践在一个退化和被破坏的网络环境中运行。

最后，美国国防部必须提高技术和创新标准，通过提高网络防御能力，保持威胁的领先地位，包括通过建立和雇用更多联合信息环境（JIE）中的防御网络体系结构。在国防部网络之外，国防部必须和民营企业一道，帮助保护国防工业基地贸易数据，并准备协助其他机构，保护美国网络和数据免受网络攻击和被网络间谍活动。

（三）战略目标三：做好准备，保卫美国国土和美国重要利益不受有重大后果的破坏性或毁灭性网络攻击

国防部门必须配合其机构间的伙伴、民营企业，以及盟军和伙伴国，威慑或在必要时击败对美国本土和美国利益造成重大后果的网络攻击。国防部必须发展其情报、警告和运作能力，在影响美国的利益之前，就削弱复杂和恶意的网络攻击。在符合所有现行法律和政策的前提下，国防部需要关于全球网络和系统、对手能力和恶意软件经纪人及市场的小型、详细、预测和可操作的情报。为了保卫自己的国家，美国国防部必须与政府的其他机构建立伙伴关系，准备进行联合的网络行动，以阻止并在必要时战胜网络空间中的入侵。国防部门侧重于构建成功完成使命所必需的手段、流程和计划。

（四）战略目标四：建立并维护可行性网络可选项，规划这些可选项的使用，在各个阶段控制冲突逐步升级，打造冲突环境

在紧张局势加剧或公开的敌对行动期间，国防部必须能够给总统提供不同种类的管理冲突升级选项。一旦有指示，国防部应该能够使用网络操作来扰乱敌人的命令并控制网络，破坏与军事有关的重要基础设施和武器功能。作为美国全套工具的一部分，美国国防部必须制定可行的网络选项，并将这些选项纳入部门计划中。美国国防部将开发网络功能，准确实现重要的安全目标，并减少生命损失和财产破坏。为确保统一，美国国防部将跨越军事运作的所有领域，规划战斗命令，并用动能作战同步网络行动。

（五）战略目标五：建立并维护强大的国际联盟和合作关系，阻止共同威胁，加强国际安全和稳定

美国国防部的三项网络任务都需要与外国盟友和伙伴密切合作。按照国际网络协议的约定，国防部将在网络安全和网络防御方面加强伙伴关系的能力建设，并在适当情况下深化业务伙伴关系。

鉴于网络资源的旺盛需求和相对稀缺，国防部门必须做出艰难选择，在美国国家利益攸关的领域，关注伙伴关系国的能力建设。未来五年，除了在其他地区致力于持续伙伴能力建

设，美国国防部将专注于参与国际社会：中东、亚太地区和关键的北约盟国。在实施这一策略的过程中，国防部将不断评估国际环境和发展创新型伙伴关系，以应对新的挑战和机遇。

四、目标实施

国防部的每一项战略目标要求各部门具体落实且量化评估。首席网络顾问，国防部部长办公室，负责采集、技术和后勤的国防部副部长办公室以及联合参谋部将配合国防部，优化和监督执行这一战略和目标，分配牵头落实部门并支持负责管理每个目标。首要责任办公室将为每一个目标制定项目计划；首席网络顾问将跟踪进度，确保每一个目标和最终的战略目标取得成功。

（一）战略目标一：建立并维护预备力量和能力，实施网络空间运作

- 建立网络力量。为了做好国防部关于网络人员的重大投资，并帮助实现这一战略目标的主要部分，国防部的第一要务是发展一支准网络特遣部队和相关的网络工作队伍。这个工作队伍将建立在三个支柱上：加强培训，改进的军事和文职征聘留用，更强的民营企业支持。

保持一个持续的训练环境。国防部要求个人和集体培训能力，以实现这一战略中所概述的目标，满足今后的业务需要。美国网络司令部将与其他部门、机构一道制定相关要求，为了使网络部队跨境和跨网络执行任务，要创建一个进行联合培训（包括练习和任务排练）、实验、认证以及评估和发展网络能力和战术、技术和程序的训练环境。

建立可行性职业发展通道。在这一战略过程中，以及在 2013 年 CMF 决议后，国防部将继续为执行和支持网络行动的所有军事人员，建立可行性职业发展通道。

利用国民警卫队和预备役。在这一战略过程中，美国国防部将把国民警卫队和预备役部门作为一种专业资源，促进创造性地解决网络安全问题。预备役部门在支持国防部的每项任务中，提供了独特的能力，包括致力于国防工业基地和商业部门。它代表了国防部针对网络反应者的重要突发作业能力。

改进文职人员的征聘和留用。除了培养高素质军事人才，国防部必须征聘和留用高素质的文职人员，包括与网络工作相关的技术人员。专为文职人员制订了周密的职业生涯规划和发展通道，使其具有同等最佳开发机遇，并有更多机会取得成功。

制定并实施与民营企业的交流方案。为了补充国防部具有文职人员身份的网络相关人员，国防部必须能够从美国最好的网络安全和信息技术公司聘请技术主题专家，在国防部内的工程和分析方面扮演独特的角色。国防部将成功实施民营企业交流方案，通过为国防部的网络空间任务设计与开发新的作战概念，为国防部带来能够衡量的利益。

支持国家行动网络教育。美国国防部将制定政策，以支持国家行动网络安全教育。与机构间伙伴、一个或更多的教育机构以及国家和民营部门伙伴合作，美国国防部将继续支持与创新型劳动力发展伙伴关系，该关系注重网络安全和网络防御的技术和政策层面。

- 打造网络运行技术手段。2013 年，为实现 CMF 的准备工作和发展可行性网络军事选项，美国国防部为总统和国防部部长开发了一个模型。美国国防部必须有可用来支持战斗命令任务行动的技术工具。主要措施包括以下内容。

开发统一的平台。根据规划要求，为集成不同的网络平台和建设具有互操作性和可扩展

性的网络功能网，国防部将制定详细的规定。此统一平台将使 CMF 进行全方位网络空间行动，以支持国家需求。

加速研究和开发。国防部将继续加快创新网络研究和开发，加强网络攻防手段建设。

美国国防部研究和发展团体，以及现有和新兴的民营企业伙伴可以为国防部和国家提供重要的发展跨越式演进技术的优势，以在网络空间中捍卫美国的利益。除了支持现有的和计划的投资，美国国防部将基础和应用研究议程的重点放在发展网络能力，扩展 CMF 能力，并壮大国防部网络人员队伍。

- 验证并不断改进网络操作的自适应命令和控制机制。近年来，美国国防部在为三个任务开发指挥和控制模型方面，取得了重大进展，但其指挥和控制模型必须定案和测试，以确保其有效性。指挥和控制模型必须支持 USCYBERCOM 和战斗命令。它必须高效和实用，并且必须在三个任务中促进努力工作的统一。
- 建立企业级网络模型和仿真能力。美国国防部将与情报机构携手合作，发展评估网络运行效力所需的数据架构、数据库、算法以及建模与仿真（M&S）能力。
- 评估网络特遣部队的能力。当面临着多个突发事件时，预估网络特遣部队的能力，实现其任务目标。

联合参谋部在美军网络司令部和其他国防部部门的支持下，将提议、收集、分析并向首席网络顾问上报一系列适当的指标，来衡量 CMF 的业务能力。这些指标将包括更新美军网络司令部应急功能状况，能力发展和熟练程度，以及访问和应急可能需要的工具。为响应这一分析结果，美国国防部将制订计划，确保 CMF 具有适当的能力，对战略环境中的变化做出灵活的反应。

（二）战略目标二：保卫国防部信息网络，保护国防部数据，规避国防部任务风险

- 构建联合信息环境（JIE）统一安全体系结构。国防部将建立国防部信息网络，以满足 JIE 统一安全体系结构。统一安全体系结构会适应并演化，以减轻网络威胁；它将帮助美国国防部发展并遵循同等最佳网络安全实践，其小型网络足迹将允许美军网络司令部、战斗命令和国防部部门维护网络威胁的综合态势感知及缓解方法。

JIE 统一安全体系结构将启用稳健的网络防御，并将关注重点从保护特定服务的网络和系统转向以统一的方式保护国防部的企业。JIE 统一安全体系结构必须用强化的网络态势感知能力开发，为响应验证要求而部署，而且能够顺应未来的防御措施。

作为 JIE 规划的一部分，国防部将开发一个框架，用于开发和将新防御技术融入美国国防部网络安全体系结构中，包括基于异常检测功能、数据分析和先进的加密方法。

- 评估并确保国防部信息网络（DoDIN）行动的联合部队总部有效性。联合部队总部-国防部信息网络将协调网络防御和降低国防企业中国防部行动和任务的网络风险。美国国防部将评估、验证和充分实施联合部队总部-国防部信息网络理念，以安全运作国防部网络、捍卫美国国防部网络和降低国防部任务的网络风险。
- 减少已知安全漏洞。国防部将开展一项工作，这项工作会减少所有给国防部网络和数据带来高风险的已知漏洞。除了零日漏洞，国防部网络和系统的最大威胁之一在于潜在的对手可以利用的已知高危漏洞。美国国防部首席信息官（CIO）将带头执

行自动修补管理能力，分发软件和配置修补程序，更新和修复，以减少国防部网络和系统上的已知主要漏洞，对抗威胁。

- 评估美国国防部的网络防御力量。国防部将评估其网络防御力量，进行综合、自适应和动态防御操作。企业级和网络保护团队（CPT）的网络维护者必须能够发现、检测、分析并减少威胁和安全漏洞，捍卫美国国防部的信息网络。
- 提高当前美国国防部计算机网络防御服务供应商（CNDSP）在捍卫和保护国防部网络方面的有效性。计算机网络防御服务供应商为国防部的网络提供网络安全解决方案，包括监测、检测和保护功能。国防部将确定当前的 CNDSP 进程是否足以保护网络免受已知的网络空间威胁，当前的 CNDSP 部队培训和装备是否足以抵御高级威胁。最后，美国国防部将确认 CNDSP 部队能否融入更广泛的网络指挥和实施控制，以及在面对存在于 CNDSP 和 CPT 保护网络和数据中的网络威胁时，如何综合实施。
- 网络防御和复原能力计划。国防部必须确定并规划保卫支持国防部重大任务的网络。国防部必须对优先资产进行谨慎评估，必须捍卫网络空间以保证完成任务，履行职能并有效地保护资产。

将网络融入任务保险评估。国防部将会把网络安全要求和评估纳入国防部任务保险方案中，并相应地更新政策。目前国防部各部门采取不同的办法衡量和评估任务保险的网络风险。美国国防部将开发一项联合任务保险评估方案，包括网络安全评估、网络安全要求和网络业务。

评估网络保护团队（CPT）的能力。美国国防部将完成 CPT 能力、功能和就业模型评估，就业模型是关于根据战斗指挥需要设置的任务保险重点。

提高武器体系的网络安全。美国国防部将评估并倡议提高当前和未来武器系统的网络安全，这样做是基于运行的要求。对于所有国防部将获得或购买的未来武器系统，国防部将要求特定的网络安全标准，以满足网络系统的要求。将更新购置和采购政策与做法，以在整个系统生命周期内促进有效的网络安全。

建立并实施持续性方案。美国国防部的各部门将确定并建立复原计划，一旦发生网络破坏和退化，可以维护它们最重要的操作持续运行。军事行动计划必须充分考虑在退化的网络环境中运作的能力；武装力量必须能够在退化的网络环境中采取军事行动，在这种环境中访问网络和数据是不确定的。各部门必须有效平衡网络风险，确保能够继续履行其在现实世界中的使命。

- 红色团队国防部网络防御。国防部已发展了成熟的“红军”，可以测试重要网络和任务系统存在的安全漏洞，并更好地准备其网络防御力量。展望未来，国防部必须将“红军”能力专注于优先网络和任务系统，以保证国防部有能力执行其最重要的任务。作为这项工作的一部分，国防部每一项主要演练都应包括网络“红军”，在被对手扰乱国防部运行的现实场景中测试美国国防部的网络防御。各部门将定期审核，以确保在结合“红军”调查结果和提高它们的网络安全态势方面取得进展。
- 降低内部威胁风险。国防取决于负责国家秘密人员的忠诚度。国防部已在技术和人员解决方案上投资，在他们能够影响美国国家安全之前，有必要确定威胁。国防部继续部署和实施这些解决方案，通过对员工队伍进行连续的网络监控和提高网络安

全培训，以改进的方法识别、报告和跟踪可疑的行为。

这项工作超越了信息技术，包括人员和可靠性问题。降低内部威胁需要良好的领导力和劳动力的问责制度。除了执行政策和协议，在他们有影响力之前，领导者将努力营造一种文化意识，以预测、检测和应对内部交易威胁。

- 为民事当局提供防御支持。根据其现有和计划中的力量结构，国防部将制定一个框架，包含民事当局的防御支持（DSCA）功能，在紧急情况下，按照指令支持国土安全部和其他机构以及各州和地方当局，帮助其捍卫联邦政府和民营企业。

国防部每年的演练计划（包括网络警卫在内），将包括与国土安全部和联邦调查局行使应急能力，可能需要紧急分配力量，在伙伴机构领导下帮助保护重要的基础设施。

这一框架将描述如何进行作战指挥，作战支援机构可以与国土安全部、联邦调查局和其他机构合作，加强一体化、培训和支持。

- 定义和细化国民警卫队在支持执法、国土防卫和民事当局防御支持任务上的作用。美国国防部将与国民警卫队合作，定义国民警卫队配合、培训、咨询和协助（C/TAA）的角色，并通过网络卫兵 16-1 来细化执行情况。根据其现有和计划的力量结构，国民警卫部队将协调、培训、咨询和协助国家和地方机构及国内重要基础设施，并为了支持国家目标，向执法、国土防卫和民事当局防御支持活动提供帮助。
- 在国防部和 DIB 公司内加强数据保护的问责和责任。国防部将确保政策和任何相关的联邦规则或已执行的合同语言要求，需要 DIB 公司向防御网络犯罪中心报告数据被窃和损失情况。

美国国防部将继续评估《防务采购法规补充条例》（DFARS）规则和相关指导，以确保它们随着时间不断成熟，以与已知的标准相一致的方式保护数据免受网络攻击对手的破坏，包括由美国国家标准与技术研究所（NIST）颁布的标准。

美国国防部将继续扩大公司威胁信息共享方案的参与度，如网络安全/信息保险计划。

因 DIB 公司的证书颁发机构清除了防御承包商站点，防御安全服务将扩大教育和培训计划，包括国防部人员和 DIB 公司承包商的材料，以提高他们的网络威胁意识。

此外，国防部情报副部长办公室将审查重要采集和技术计划的当前分类指南的充分性，以保护承包商网络上的信息。

- 加强国防部采购和采集网络安全标准。为了保卫美国国防部网络，国防部必须加强国防部网络采集和采购项目的网络安全要求，将网络安全标准纳入合同车辆的研究、开发和采购中。美国国防部将指定额外的行业网络安全标准，以满足国防部任意部门的采购项目。
- 建立采集、情报、反间谍、执法和行动团队的协作，以防止、减少和应对数据丢失。美国国防部将建立联合收购保护和开发单元（JAPEC），连接情报、反情报和执法人员与采集程序经理，防止和减少数据丢失及被盗。美国国防部将对网络间谍活动和盗窃进行全面的风险和损失评估，以告知要求、采集、方案以及行动的反情报过程。

美国国防部首席信息官，与国防部采集、技术和后勤副部长办公室合作，将评估并更新特定信息系统安全控制，这是《防务采购法规补充条例》的基础，在 NIST 和 DFARS 标准范围内规定防御承包商。

为保障关键程序和技术，国防部将与企业合作，发展预警能力和建立分层的网络防御。

最后，国防网络犯罪中心，国防部部长办公室的首席网络顾问，国防部采集、技术和后勤副部长办公室将与服务损害评估管理办事处协作，简化风险和损害评估进程，更好地告知维持、修改或取消被渗透的程序的决定。

- 利用国防部反谍报能力来抵御入侵。军事部门和国防部情报副部长，与首席网络顾问一起协商，制订战略提交国防部部长批准，强化军事部门反间谍机构的能力和权威，识别、归类并抵御网络入侵者。

在提高洞察、挫败和击败网络间谍活动能力方面，反情报当局有着独特的优势。该战略将指定国防部的反情报机构如何更加有效地与更广泛的美国情报和执法机构合作，调查及操作人员和技术，以遏制针对美国及其盟友和伙伴的网络知识产权窃取。

- 支撑政府整体政策和处置能力，打击窃取知识产权。国防部将继续与美国政府的其他机构一道，对抗通过网络窃取知识产权所带来的威胁。

（三）战略目标三：做好准备，保卫美国国土和美国重要利益不受有重大后果的破坏性或毁灭性网络攻击

- 继续发展情报和预警能力，预测威胁。为了保卫国家免受网络攻击，美国国防部将更广泛地与情报机构合作，增强敌情收集能力，在对美国本土和美国利益产生影响前，扰乱网络攻击。为了满足作战指挥的应急需要，国防部将加强重要对手情报的人力投入和技术网络。为了在网络空间中有效运作，国防部要求，在潜在行动的各个阶段，感知网络情报、预警和共享态势。所有的情报收集都将依法行事。
- 培养和锻炼保卫祖国的能力。国家特遣部队和国防部的其他相关部门，将培训重要的跨部门组织，并与其合作，开展网络行动，保卫国家免受网络攻击。此外，国防部将通过在各级部门定期演习，以及紧急和有计划的实战演练完善应急程序。
- 网络行动程序。建立伙伴关系，保卫国家。国防部将构建一个与其他政府机构的合作框架，开展保卫国家的行动。美国国防部将与联邦调查局、中央情报局、国土安全部和其他机构建立关系并整合能力，为总统提供范围最广的选择，应对可能对美国造成严重后果的网络攻击。

对国防部保卫国家的能力，进行年度全面审查。国防部对于其保卫国家、抵御有严重后果的网络攻击的任务的要求和能力，会随着时间的推移而变化。在年度审查的基础上，国防部将对其任务的现有和所需能力，进行深入审查。

作为这项审查的一部分，美国国防部将明确新要求，并查明要追赶的差距和措施。

- 制定保卫美国重要基础设施的创新办法。美国国防部将配合美国国土安全局改善先进网络安全服务项目，并鼓励其他重要基础设施实体参与，特别侧重于提高国防重要基础设施参加者的数量。
- 开发自动化信息分享工具。为了提高共享态势感知，美国国防部将与国土安全局和其他机构合作，制定连续、自动化、标准化机制，与每一个美国政府的重要伙伴、重要同盟和合作军队、国家和当地政府及民营企业分享信息。此外，美国国防部将与其他美国政府机构和国会一道，支持美国政府和民营企业之间共享信息的立法工作。

评估美国国防部的网络威慑态势和战略。建立国防科学委员会的网络威慑特别小组，美国战略司令部（USSTRATCOM）将配合联合参谋部和国防部部长办公室，评估国防部门的能力，阻止特定国家和非国家行为者在美国本土和损害美国的利益方面进行有重大后果的网络攻击，包括生命损失、重大破坏财产或对美国外交和经济政策利益产生重大影响。

在开展分析时，美军战略司令部必须确定国防部是否具备溯源和遏制重要威胁所需的能力，威胁来自这类攻击行动，并推荐特殊措施，美国国防部可以采取这些措施提高其网络威慑态势。必须谨慎关注，防止非国家行为者可能会走出传统威慑框架，可能对美国利益造成较大的威胁。

（四）战略目标四：建立并维护可行性网络可选项，规划这些可选项的使用，在各个阶段控制冲突逐步升级，打造冲突环境

将网络可选项纳入规划。为了满足由部队部署指南、作战指挥计划和其他战略指导文件所定义的战略结束状态，国防部将与美国政府机构以及美国的盟友和合作伙伴一道，将网络可选项纳入作战指挥规划之中。

加快将网络要求纳入规划。国防部将加快将网络要求融入作战指挥的计划。计划必须说明和定义针对目标的特定网络空间影响。为推动这项工作，联合参谋部将与美军战略司令部一道，将要求同步和纳入规划之中，并在网络特遣部队的结盟、部署、委派和分配方面，向国防部参谋长联席会议主席提供建议。

（五）战略目标五：建立并维护强大的国际联盟和合作关系，阻止共同威胁，加强国际安全和稳定

- 在关键区域建立合作能力。根据其现有和计划的力量结构，国防部将与关键的盟友和伙伴一道，建设伙伴能力，帮助保护重要基础设施以及国防部任务和美国利益所依赖的关键资源。国防部将与美国政府的其他机构一起定期工作，建设合作伙伴能力。优先区域包括中东、亚太地区和欧洲。

支持中东地区盟友和合作伙伴强化网络和系统及自我恢复能力。作为网络对话和伙伴关系的一部分，美国国防部将与重要的中东盟友和伙伴一道，提高它们的能力来保护其军事网络以及美国利益所依赖的重要基础设施和关键资源。重要举措包括改善信息共享，建立网络威胁统一认识，制定多方网络防御态势评估和网络专业知识的合作办法。

支持东北亚盟友的网络和系统强化及自我恢复能力。作为与亚洲盟国的更广泛网络对话的一部分，美国国防部将与重要盟友和伙伴一道，提高其能力，以保护它们的军事网络和美国及其盟国的利益所依赖的重要基础设施及关键资源。

以符合国防部《国际网络空间安全合作指导意见》的方式在亚太地区建设新型战略伙伴关系，国防部将与亚太地区的重要盟国一同建设网络能力，使美国和盟国利益的风险最小化。

与重要的北约同盟国一道减少针对国防部和美国利益的网络风险。国防部将通过与重要的北约同盟国进行防务磋商，发展这些伙伴关系。

美国国防部在建立联盟和伙伴关系的同时，将保持灵活性和敏捷性，以在战略环境中最好地应对变化。

- 开发针对破坏性恶意软件扩散的解决方案。国家和非国家行为者会寻求获得破坏性

恶意软件。破坏性恶意软件向敌对行动者的无节制传播，使国际体系面临着重大风险。通过与国务院和美国政府的其他机构，以及美国的盟友和伙伴合作，国防部将借鉴最佳做法，防止破坏性恶意软件在国际体系内的扩散。除了国际体制和最佳做法，美国政府还拥有一系列国内出口管制制度，用于管理防止扩散的两用技术。

- 与有能力的国际伙伴合作，规划和培训网络操作。在这一战略过程中，美国国防部将加强其国际联盟和伙伴关系，发展联合能力，为支持作战指挥计划获得网络影响。
- 加强美国与中国的网络对话，增强战略稳定。通过这一战略过程，作为中美防务磋商会谈和相关对话的一部分，比如网络工作组，美国国防部将继续与中国保持商讨，增进两国在网络空间中军事原则、策略、角色和任务方面的理解和透明度。这项工作的目标是减少误解和误判的风险，这些都可能造成情况加剧和不稳定。美国国防部将支持美国政府努力加强信任建设措施，为美中两国关系带来更高层次的信任。

五、战略管理

要实现这一战略所述的目标，需要对网络部队、人员和机构、组织和功能做出艰难的抉择。国防部在实施这一战略过程中的财务选择，在几年内，将产生国家和全球影响，国防部必须以有效和高效益的方式运行，保证其投资获得最佳回报。为此，美国国防部将追求以下管理目标，以管理其网络活动和任务。

- 为国防部部长设立首席网络顾问办事处。在 2014 年《国家国防授权法案》（NDAA）中，国会要求国防部为国防部部长指定一名首席网络顾问，审查军事网络空间活动、网络特遣部队和进攻性及防御性网络行动和任务。此外，首席网络顾问将管理为国防部的企业指定的国防部网络空间政策和战略的发展。
- 2014 年 NDAA 还规定，这位首席网络顾问要汇总网络专业知识和关键组织的观点，打造一支拥有关键队员的部内团队，以确保有效治理国防部内部的网络问题。FY14NDAA 为首席网络顾问确定的职责不应被解释为，在与网络相关的职责和权利方面，能够影响国防部办公室采集、技术及后勤副部长，政策副部长，情报副部长，人事和准备副部长或者任何其他主要工作人员助理（PSA）的现行职责和权力。
- 建立一支部内团队。首席网络顾问将通过网络投资和管理理事会（CIMB），与美国国防部部门审查国防部的网络管理工作。CIMB 将是一个同步、协调和项目管理的论坛。它不会复制现有的方案和预算机制，或干扰先前定义的主要工作人员助理的角色及权利，也不会以任何方式干扰军事指挥链；相反，它将提供一个单一论坛，以整合网络倡议，它将通过完工进行项目管理，精简国防部的网络治理结构。首席网络顾问将与国防部采集、技术及后勤副部长和联合参谋部共同打造美国国防部代表的内部团队，在这项工作中支持 CIMB。
- 建立一个高级行政论坛。高级行政论坛隶属于并向 CIMB 汇报工作，它将提供关于关键网络问题的首次高级别协作。高级行政论坛将向 CIMB 推荐行动方针，并将与其他安全协调员办公室和联合参谋部的管理机构协作，以促进工作统一和在适当层次上解决管理问题。

如果在计划和预算审查过程中，预算或财务出现问题，首席网络顾问将使用高级行政论坛和 CIMB 向代理的管理行动小组或其他财政和预算组织协调建议，如果合适即通过问题小

组检查选择和方案。

- 提高网络的预算管理。美国国防部将研发商议的方法，更加透明和有效地管理国防部网络运行预算。今天，用于网络方面的资金遍及美国国防部的预算，涉及多方部署、预算明细、程序环节和项目这些方面，包括军事情报程序（MIP）。此外，代表美国国防部，情报副部长要确保所有国家情报程序（NIP）投资配合与支持国防部的任务。

美国国防部网络预算的遍及性给国防部的有效预算管理带来了挑战；美国国防部必须研究一种新方法，管理跨项目资金，以改善任务效果，并实现管理的高效率。

- 制定美国国防部网络操作和网络安全的政策框架。为符合总统的指导意见，美国国防部将配合和简化其网络运行和网络安全策略管理，以及在当前文件中需要修订、已查明的差距、重叠、接缝、冲突和领域。这一工作将有助于把国家和部门的指导和政策转化为战术行动。有必要把现有文档中的冲突解释清楚，这些冲突可能会使网络操作和网络安全复杂化。
- 对美国国防部的网络功能进行终端到终端的评估。美军网络司令部将领导态势综合运行评估。通过与国防部部长的首席网络顾问，国防部采集、技术和后勤副部长办公室，以及海岸和方案评估理事办公室相配合，美军网络司令部将通过 CIMB 向国防部部长提供短期和长期建议，这些建议涉及组织结构、指挥和控制机制、工作规则、人员、功能、潜在运作差异。这一态势评估的目标是为未来的运作环境提供一个清晰的认识，关键利益相关方的意见，以及规划和行动的战略优先事项、选择和资源。

六、结论

我们生活在一个对美国利益的网络威胁日益增长的时代。国家和非国家行为者扬言对美国进行破坏性和毁灭性攻击，进行网络知识产权窃取，削弱美国的科技和军事优势。我们在网络空间中脆弱不堪，需要政府和民营企业领导人及组织采取紧急行动。

自从 2011 年制定其首个网络策略以来，国防部已经在建设网络能力、发展组织和计划，以及培养捍卫国家和其利益的必要伙伴关系上取得了重大进展。还有很多必须要做的事情。出于这一战略所述的目标，必须分配和管理适当的资源，以确保取得进展。

这一战略为实现变革提出了积极、具体的计划。对于美国国防部来说，要成功地完成其使命，捍卫美国及其在网络空间的利益，整个部门的领导人必须采取行动，实现上述各项目标。他们还必须为其组织负责。由于网络和计算机代码的性质，不能依靠单一的组织来做这项工作。成功需要国防部和美国政府机构与民营企业以及美国的盟友和伙伴密切协作。

战略环境可能变化很快，特别是在网络空间中。在这项工作中，我们必须保持动态、灵活和敏捷。我们必须预见到新兴威胁，发展新的能力建设，并确定如何加强我们的伙伴关系和规划。一如既往，我们的军警人员和文职人员将是我们最大、最持久的力量和源源不断的灵感。通过共同努力，我们将帮助保护和捍卫美国及其在数字时代的利益。

报　告　篇

网络空间安全：迫在眉睫的危机

一、执行摘要

当前，对于美国通信、商业和管理方面涉及的实体性基础设施而言，信息技术（IT）基础设施显得至关重要，但是，它却非常容易受到恐怖分子和罪犯的攻击。通过部署健全的安全产品并贯彻良好的安全实践，民营企业在保障国家的信息技术基础设施安全方面发挥了重要作用。但是，通过支持研发能够强化这些产品和实践性能的网络空间安全技术，联邦政府也可以发挥关键作用。美国总统创新技术咨询委员会（PITAC）认为：联邦政府需要从根本上改善这种网络空间安全途径，才能更好地履行这方面的责任。

（一）背景

在过去十年里，美国的信息技术基础设施已经发生了引人注目的转型。连接各种信息技术系统的网络应用开始呈现爆炸性的增长，使其能够以相对容易的方式获取信息，从而实现在更大距离范围内进行通信并控制这些系统。由于通过这些网络系统可以大大提高生产效率并实现全新性能，它们已经融入大量的民用设施中，包括教育、商业、科学、工程和娱乐等。实际上，它们已经融入国家关键基础设施的各个层面，包括通信、公用事业、金融、运输、执法和国防等。的确，这些领域现在无不依赖于潜在的信息技术基础设施。

同时，互联网引起的这场革命也助长了那些破坏分子的气焰，使其有能力仅用一台计算机以识别和侵入对方薄弱点的知识，就能形成远程破坏。今天，敌方有可能在几分钟的时间内入侵世界各地的数百万台计算机，再利用这些计算机来攻击国家的关键基础设施，渗透到敏感系统或者窃取宝贵的数据。攻击次数的增加，源于互联网的巨大成长，如今国家应对这些攻击的年度支出都在数十亿美元。而且，这些破坏分子正在快速占领我们的国土，大量的受损网络及其造成的财务损失就是明证。

除了经济损失之外，网络也给我们的国家安全带来了诸多显而易见的风险。除了对我国境内的关键目标进行潜在攻击之外，我们国家的防御系统也正在面临风险，因为我国的军队越来越依赖于无所不在的通信及其网络。预计全球信息网（GIG）每年的支出都在 1000 亿美元，其目标是通过互连武器、情报和军事人员来改善军用通信能力，它代表了一种关键性的网络。因为军用网络能够和民用网络实现互联，或者可以使用类似的硬件或者软件，所以它们很容易成为攻击对象。因此，从本质上而言，民用领域和军用领域内的网络空间安全是相辅相成的。

尽管网络空间安全产生的巨大成本仅在最近有所显现，但是国家的网络空间安全问题却已存在数年之久，并且在未来数年仍将给我们造成损失。我们需要从数十年的失败中吸取教训，进而开发安全协议和惯例，以保护我国的信息技术基础设施，还要充分地培训和教育大

量相关专家，以便有效地利用这种机制。在隔离薄弱点方面，今天我们所部署的短期补丁和应对措施是有帮助的，但是并不能适当地解决核心问题。因此，我们需要开展基本的、长期的基础性研究来开发全新的途径保护网络空间安全。在情势恶化以及惰性成本扩大之前，我们很有必要采取行动措施。

（二）结论和建议摘要

总统信息技术咨询委员会对网络空间安全提出了建议，并基于这些建议得出了结论，现摘要如下。

问题 1：联邦政府对于民用网络空间安全基础研究的拨款支持水平

因为市场规律让民营企业投资远离研发领域，应用现有的技术来开发适销产品赚取利润，所以，对于网络空间安全的长期、基础性研究，要求联邦政府给予重大投资支持。但是，联邦政府对于网络空间安全研究的拨款，已经从长期的基础性研究转向短期研发，从民用研究转向军用和情报用途。这些领域内的研究通常属于国家机密，因此，其研发成果很难被用于保护政府和民用领域内广泛部署的民用信息技术基础设施和商用现货产品。在美国国防高级研究计划署（DARPA）和国家安全局（NSA），这些变化尤其显著；其他机构，如美国国家科学基金会（NSF）和美国国土安全局（DHS），还没有填补现有的空白。而在最需要的时候，民用网络空间安全基本研究领域的投资却已开始下滑。

美国信息技术咨询委员会发现：联邦政府的研发预算不能为民用网络空间安全领域内的基础研究提供足够的拨款，建议美国国家科学基金会（NSF）每年在这个领域内增加 9000 万美元的预算支出。其他机构也应对民用网络空间安全基本研究实质性地增加拨款，尤其是美国国防高级研究计划署（DARPA）和美国国土安全局（DHS），应当划拨这笔款项，适当地关注“优先考虑的网络空间安全研究”中列出的十个重点领域。根据国家未来的网络空间安全发展态势，拨款可以进一步增加。

问题 2：网络空间安全基本研究机构

改善美国的网络空间安全态势要求训练有素的合格人员投入研发、部署和集成全新的网络空间安全产品和实践中。相对于面临的巨大挑战，美国境内训练有素的合格人员数量很少。目前，按美国信息技术咨询委员会估计，在美国的学术机构中只有不到 250 位较为活跃的网络空间安全或者网络保护专家，其中多人在此领域都缺乏正式的培训或者丰富的专业经验。造成这种状况的部分原因是，网络空间安全历来都是计算机科学和工程研究机构的重点研究领域。由于对长期民用网络空间安全研究领域的投资都是不充分和不稳定的，使得这种情况进一步恶化，而大学机构却有赖于这些研究来吸引和留住教职人员。

美国信息技术咨询委员会发现：美国的网络空间安全研究机构规模太小，不足以支撑为美国提供保护的网络空间安全研究和教育计划。美国信息技术咨询委员会建议：联邦政府应当努力在研究性大学招聘和保留网络空间安全研究人员和学生，以期在十年后将民用网络空间安全基本研究机构的规模至少扩大一倍。尤其是，联邦政府应当增加对于民用网络空间安全方面的稳定拨款，并且应当支持相关计划，使得研究人员能够从其他领域转入网络空间安全研究领域。

问题 3：把研发努力转化为国家有效的网络空间安全力量

技术转让可以使联邦政府支持的研发成果融入广泛应用的产品中去。在联邦政府支持的信息技术研发成果转化为民营企业内广泛应用的产品和最佳实践方面，美国拥有悠久的成功

历史，甚至催生了全新的十亿级产业。尤其是在网络空间安全领域，技术转让面临着巨大挑战；但是，因为无论良好的网络空间安全产品价值还是消费者，都依赖于降低成功攻击的可能性——我们很难对短期投资回报进行量化。

美国信息技术咨询委员会发现：当前的网络空间安全技术转让努力并不能够成功地将联邦研究投资转化为民用领域内的最佳实践和产品。因此，美国信息技术咨询委员会建议联邦政府应当加强网络空间安全技术转让合伙企业和民营企业之间的合作。尤其是，联邦政府应当重点推动各种指标、模型、数据库和测试台的研发，以便对全新的产品和最佳实践进行评估；民营企业应当在展示全新网络空间安全成果的年度跨界会议上给予联合赞助；对于拥有前瞻性研发理念或者技术的研究人员的技术转让努力（与产业合作）给予拨款支持；鼓励联邦政府支持作为研究人员、实习生或者顾问的研究生和博士生研究人员获得行业经验。

问题 4：联邦网络空间安全研发协调和监督

联邦政府当前采取的网络空间安全对策产生的一个关键问题是，政府对于网络空间安全研发行业开展的协调效果不佳。整个机构内的研究议程和计划没有实现系统性的协调，结果导致各个机构对于彼此的计划和职责产生误解，以至于忽视优先考虑的重点任务。如果协调不足，个体机构就会专注于其自身的任务，而忽视整个国家的全局性需求。因此，联邦政府只有通过不断增强其协调能力，才能自发性地增强和扩大网络空间安全研究机构，使其更为有效地实施研发成果。

总统信息技术咨询委员会发现：由于协调和监管不佳，导致当前联邦政府的整个网络空间安全研发工作重点不突出。为了对这种情况进行整顿，总统信息技术咨询委员建议：关键信息基础设施保护署（CIIP）跨界工作组应当重点负责协调联邦网络空间安全研发工作。在网络和信息技术研发计划中，应当强化和融合这种工作组的职责。

二、网络空间安全：国家的重要议题

（一）在充斥危险的世界里相信系统的力量

当前，美国的信息技术基础设施依然能够依靠美国的技术创新（例如个人计算机和互联网）而得到不断进化，它已经构成一张巨大的计算机网络（从超级计算机到手持设备），并且互联网还催生了社会各个领域赖以生存的高速通信、信息访问、高级计算、处理和自动化程序系统等。这种基础设施通过各种方式和互联网实现连接，它体现了互联网开放、创新和善意的结构属性。

这些识别属性使得美国信息技术基础设施成为强烈吸引世界范围内破坏分子和犯罪分子的攻击目标。美国信息技术咨询委员会认为：恐怖分子必然会如法炮制，充分利用那些包括美国尚未明确识别或者处理弱点在内的各种薄弱之处。管理美国关键设施、基础设施和基本服务行业的计算机也会成为攻击目标，从而引发系统内故障；而且，在世界任何地方的人都可以通过互联网频繁地访问这些计算机。

（二）信息技术基础设施属于“关键”设施

大多数美国人都了解并使用信息技术基础设施元件。主要是连接到互联网的台式计算机，以便收发电子邮件和即时信息、交流和下载声音和图像、在线购物、进行信息研究、互

动游戏，甚至使用网络电话。美国也在努力研发信息技术，从而驱动产业和政府的日常运行，并且依赖于不同规模、不同功能的组织机构，包括设计、生产、制造、存货、销售、工资发放、信息存储和检索、教育和培训以及研究和开发等。事实上，经济学家会将美国在过去十年内大大提高的生产率归功于信息技术的成功应用。

1. 美国的信息技术基础设施非常容易受到恐怖分子和犯罪分子的攻击

越是难以察觉，当然就越难以理解，这就是现实。计算机、大容量存储器、高速网络，以及诸如路由器和转换器、系统、应用软件、内置和无线设备等网络元件，甚至是互联网本身等这些技术，如今对于美国的所有关键性基础设施而言也至关重要。计算机系统控制和管理着美国的电厂、大坝、北美国家电网、空中交通管制系统、食品和能源分配系统、金融系统等。这些敏感性的物理装置和程序对信息技术基础设施的依赖，使得这些信息技术基础设施自身变得十分重要，尤其是对于保护国家利益而言变得更加重要。

例如，发电行业就依赖于广泛的信息技术系统和性能。而在其他行业内，电力公司会执行业务管理系统来满足行政和信息服务要求。但是电力行业也会使用更多的信息技术。它依赖于数据采集和监视控制系统来采集关于系统运行的信息，帮助调度和控制发电，优化电力生产，对于不断变化的电力需求和控制分配做出响应，并对电力公司系统内各种不同的发电和存储设施进行协调。数据采集和监视控制系统还被越来越多地用于将电子公司融入地区或者国家电网，以便优化电力生产，最小化生产和配电成本，并提供备份服务。这就要求将通常使用的专用网络连接到互联网。能够瘫痪关键互联网节点的网络攻击，还可以破坏电力网络的通信系统。如果专用网络中的实体部分遭到破坏，那么攻击者就可以直接控制数据采集和监视控制系统及其数据和运行。

2. 当前，计算机、网络和网络元件是美国所有关键基础设施的基本构成要素

今天，互联网也被用于管理商业和政府部门所提供的基本服务，如电子金融交易、执法调度和支持、应急响应、社区警戒和军事通信等。例如，不管是与消费者互动还是银行间运作，银行都必须依赖于广泛分布的互联网和信息服务。为了确保最为敏感系统的可靠性和安全性，银行业和电力行业都会使用专用网络，但是这些网络很容易遭到网络攻击，致使网络节点瘫痪，以至于无法访问数据和服务。例如，这些共享的互联网连接，甚至不必直接连接到互联网，蓝宝石蠕虫（Slammer）病毒程序就可以乘虚而入，进而造成主要银行的自动取款机系统和航空公司的计算机系统瘫痪。

在国家突发紧急情况时，我们有必要使用国家的通信基础设施来进行应急响应协调。今天，至关重要的基础设施非常容易造成各种负面服务攻击，包括释放简单病毒和蠕虫，以破坏互联网通信；或者通过破坏服务器侵入调制解调器，进而渗透电话网络的关键元件，实施更为复杂的攻击（如 911 服务）。后者告诉我们：攻击者怎样充分利用系统弱点（如互联网）来攻击综合分布系统（如电话网络）。

这些案例告诉我们：计算系统和计算机通信已经成为当今美国各个活动领域内不可或缺的组成部分。这些系统以高度复杂的方式彼此互连彼此依赖，但是通常也非常脆弱。

（三）无所不在的互连性=普遍性的弱点

如今，互联网连接着世界范围内 3 亿多台计算机，互联网的设计基于相互信任的精神。

然而，无论是网络通信协议还是管理网络连接的计算系统（节点）软件都不能避免遭受攻击。诚然，今天互联网使用的协议源于联邦政府 20 世纪 60 年代在阿帕网实验中研发的协议。当时，只有为数不多的研究人员使用阿帕网，并且他们相互信任，不会给对方造成破坏。通过阿帕网转入互联网的民用网络（如美国国家科学基金会网络），没有在其系统软件或者网络协议层面集成任何安全技术。

1. 无所不在的互联是广泛利用弱点的主要渠道

无所不在的互联，首先由互联网及其扩展局域网、广域网、无线和混合网络展现出来，已经催生了全新的产业，复兴了落后的生产力，为研讨和教育创造了全新的途径，开启了全球合作科学和工程发现的空前时代。这的确是好消息。坏消息是，这种无所不在的互联网也成为攻击者广泛采用的主要攻击渠道。尽管在最近几年里，美国努力在计算机系统、网络和软件中集成更多安全元件，但是，诸如恐怖分子、敌对国家、有组织犯罪或者恶意黑客等敌对势力，都可以通过远程扩散对我们造成国家级或者国际级的破坏效应。

2. 敌对势力的行为可以远程扩张

在过去几年里，诸如红色代码[1]蠕虫病毒程序（丑化全球网站以及/或者发动分布式拒绝服务攻击[2]）和蓝宝石蠕虫病毒程序（2003 年 1 月，对美国银行的自动取款机网络造成了严重破坏）等，预计已经造成了数以十亿计美元的损失。

美国国防部通过从互联网上断开无保密网络（无保密互联网协议路由器网络）的方式，回应红色代码蠕虫病毒程序造成的攻击，以保护系统免遭传染。这种防护性的措施瘫痪了工程师军用公司对美国密西西比河的水闸控制，因为无保密互联网协议路由器网络的主要用途是通过互联网传输水闸命令。

通过使用笔记本电脑和无线电发射器，先前的海外废水系统承包商就能够获得数百套控制系统命令，以便管理污水和饮用水。在两个月的时间里，他们蓄意通过废水系统排放了成百上千加仑的有毒泥浆。

如今，许多公司正在受到网络敲诈者的攻击，他们要求没有受到攻击的公司给予回报。2004 年，卡内基・梅隆大学《信息周刊》报道：在被调查的 100 家公司里，有 17%都在一定程度上变成了网络敲诈的攻击目标。

对于互联网用户而言，身份盗用问题迅速增多。偷窃用户身份最简单的一种方法被称为“网络仿冒”，这种技术可以使用假冒的电子邮件信息和欺诈性网站，从而诱骗收件人泄露个人财务数据。消费者联盟预计：美国有 1%的家庭成为了这种攻击的受害者，2004 年上半年造成的损失在 4 亿美元左右。

（四）软件是一个主要弱点

网络连接可以为攻击者提供“上门”运输，但是计算机配置软件中存在的弱点实质上会恶

[1] 通过扫描互联网传播的大部分网络蠕虫，可以识别易受攻击系统，通过安装它们感染这些系统。可参考以下网址：http://www.computereconomics.com，2004 年 9 月。

[2] 拒绝服务攻击会覆盖有人工服务要求的目标，致使其不能提供合法服务。分布式拒绝服务攻击会在众多计算机中分布人工要求来源，因此会大大增加阻碍连接任务的复杂性，以消除特定来源的人工要求。分布式拒绝服务攻击的计算机通常是真实攻击者未觉察到的代理。

化网络空间安全问题。正如总统信息技术咨询委员会在 1999 年发布的报告[1]中指出的那样，已经形成规范的软件开发方法并不能提供信息技术基础设施所要求的高质量、可靠、安全的软件。软件开发还没有成为一门科学，或者说严密的学科，开发过程在很大程度上不可控。今天，和癌症一样，脆弱的软件容易遭到入侵和篡改，从而对先前健康的软件造成破坏，被传染的软件还可以自我复制，并且在网络中存在，对其他系统再造成破坏。和癌症一样，对于没有经验的人来说，这些破坏过程是无形的，尽管专家意识到它们的威胁还在不断增加。和应对癌症一样，预防性措施和研究是很关键的，前者是为了将今天的破坏降低到最小限度，而后者是为了建立知识和能力基础，以便协助明天的网络空间安全专家降低风险，并将长期破坏降低到最小限度。

今天，由于错误或者低劣的实践而引入的软件弱点，成为了一个严重问题。将来，当敌对势力（包括国内外的敌对势力）发展出越来越高级的能力，进而能够将恶意代码插入关键软件时，我国甚至可能会面临越来越具有挑战性的问题。

（五）攻击和弱点都在快速增长

今天，我们所面临的威胁出现了明显增长。在组织机构和个人之间，关于网络空间安全事故的频率、影响、范围和成本的大部分指标和研究，都是为了应对这些不断增长的威胁和各种攻击。数据显示：攻击总数——包括病毒、蠕虫、网络欺诈以及公司内部人士攻击——每年都在以 20%的速度递增，许多攻击类型甚至增长了一倍。例如，德洛伊特“2004 全球安全调查”显示，83%的金融服务机构都在 2003 年经历了系统破坏，比 2001 年的比例增加了一倍多。而且，安全事故的报道态度比实际情况保守得多。大型组织机构几乎没有太多动机（不利因素除外）在公共论坛上报道事故。通常，网络攻击的目标会受到关注：如果受害信息广泛泄露，就会动摇公众对于它们运营的信心，而不是吸引其他攻击者。

以技术为导向的指标清晰地反映了网络攻击比例的快速增长。例如，国际计算机安全协会实验室报告称：每月受到病毒传染的个人计算机比例已经从 1996 年的 1%增长到了 2003 年的 10%。美国赛门铁克软件公司发布的互联网安全威胁报告[2]称：从 2004 年 1 月到 6 月，受到“蠕虫军团”破坏的最新主机比例从不到 2000 台/天，增长到了 30000 台/天。当受损主机混入“蠕虫军团”时，它们可以被用做针对给定目标启动拒绝服务攻击的平台，或者在所有人以及操作者不知情或者不许可的前提下，向其发送“垃圾”电子邮件。

较大组织机构内的趋势也令人不安。例如，在过去十年里，经历病毒灾难的组织机构（被定义为同时受到 25 次传染或者更多传染冲击的组织机构）比例几乎每年都在增长，2003 年，有 92%的组织机构报告了这样的事故。美国赛门铁克软件公司报告称：被全球 100 强控制的网络中，有 40%的网络会被利用，进而形成敌对的蠕虫流量，尽管这些公司已经采取了各种防护性措施。根据国际计算机安全协会实验室的数据：从重大的病毒事故中恢复过来所需的成本、停工期和天数在过去 9 年内都呈现上升趋势。

同时，识别系统和网络脆弱点的数量也在攀升。卡内基·梅隆大学的计算机应急响应小组协调中心（CERT/CC）报告称：2004 年公布了 3780 个全新的电子弱点，比 1995 年增加了 20 倍。一旦发布，大部分的细节弱点都会被歹徒用于开展攻击或者开发攻击工具和技术，因此迫使用户和组织机构确保他们防卫的充分性。美国赛门铁克安全威胁报告指出：2004

[1]《信息技术研究：投资未来》总统信息技术咨询委员会，1999 年 2 月。

[2] 请参考以下网址：http://enterprisesecurity.symantec.com/content.cfm?articleid=1539。

年上半年，弱点公共泄露和泄露相关漏洞之间的平均时间为 5.8 天。

事实上，许多信息技术系统设计继续融合相关性能，使得这些系统容易受到攻击。在某些案例中，系统设计可以达到高级的程度，因此在部署之前不能理解其中的弱点。在其他案例中，可以将某些弱点融入系统中，因此开发者缺乏技术知识或者不能执行最佳实践。在这份简短的报告中，总统信息技术咨询委员会可以仅依赖几个案例，为读者提供信息技术系统弱点。但是，很明显，当计算机、手机和嵌入式系统在全球扩散时，或者当扩散“通常运行”高速或者宽带连接时，如果没有采取行动，信息技术弱点就会变得更为严重，这样一来，攻击扩散就会变得更快，甚至会比成为规范的临时连接低带宽调制解调器威力更强大。

（六）数不清的补丁并不是答案

计算机科学家日益达成了广泛共识：修补和篡改网络、计算系统和软件进而“增加”安全性和可靠性，在短期内是有必要的，但是在应对美国网络空间安全需求方面还不充分。在白宫科学委员会发表声明之前，计算机安全专家和总统信息技术咨询委员会成员尤金•斯帕福德证实：安全问题并不是那么容易解决的问题，这就使得我们的总体任务变得更为复杂。今天我们正使用的软件和硬件都是由那些接受很少或者根本没有接受过安全培训的人员部署的，并且使用的设计方法不安全，开展的测试并不规范。这些软件和硬件被安装到满是缺陷的基础设施之中，并且由风险意识不足的工作人员来操作。因此，如果在未来数年[1]内，我们继续看到非法入侵、毁损和病毒的不断增长，谁也不会感到意外。

即使我们在全球各地已经使用了所有已知的最佳安全实践，我们的信息技术基础设施可能也没有那么安全。但是斯帕福德教授发出评论建议称：即使所有的最佳实践都完全部署到位，如果缺乏任何根本的全新途径，我们仍旧会需要数不清的补丁，并且“堵塞堤防的漏洞”。

（七）根本上全新的安全模型、所需方法

我们迫切需要增加对于短期修补的关注度，还要包括在较长时间范围内研发设计安全系统的最新方法。处理较长期网络空间安全要求严格执行基础研究计划，从而探索科学并发展必要的技术以保障计算和网络系统及软件安全。基础研究的特征是其广泛潜力，而非具体应用，包括高瞻远瞩、高回报的研究，从而为技术进步提供基础[2]。

截至目前，大量的网络空间安全研究都是基于边界国防的概念。在这种模型里，在信息系统或者网络“内部”的元素可以得到保护，以免受到试图渗透访问或者控制其数据和系统资源的“外部”攻击者的攻击。但是，一旦破坏其边界（无论是属于技术劣势，如软件弱点；还是操作劣势，如被贿赂或者欺骗而泄露其口令的雇员），攻击者就拥有完全的行动自由，并且可以破坏网络中连接的任何系统，其所耗成本可能和仅破坏一套系统无异。

边界国防战略的这种劣势已经变得非常显著，令人痛苦。但是，这并不是此模型遇到的唯一问题。由于连接到网络的无线和内置技术的扩散，以及网络“系统中的系统”的复杂性不断增加，“外部”和“内部”的崩溃特征有所不同。

网络空间安全中更为现实的模型所涉及的一种元素为相互怀疑原则：每套系统或者网络元件通常会怀疑其他元件，如果要访问数据和其他资源，必须不断重新授权。更为普遍的情况是，网络空间安全会成为任何大型、复杂系统或者网络设计过程中不可或缺的组成部分。

---

[1] http://www.house.gov/science/hearings/full/oct10/spafford.htm。

[2] 根据美国国家研究委员会发布的《国防部基础研究评估》改编，美国国家学术出版社，2005 年。

通常情况下，我们有必要使用安全补丁来修复某些安全问题，但是最终却无法替代能够实现最低限度入侵的系统范围内的端到端安全。

（八）联邦研发的核心作用

“美国国家网络空间安全空间战略”声称：民营企业在网络空间安全方面可以发挥最为重要的作用。总统信息技术咨询委员会同意这个结论，因为它可以通过相对短期的努力来改善当前系统和网络的安全程度。但是，联邦政府也可以在其中发挥至关重要、不可替代的作用。在数字革命的较早阶段，联邦政府需要对基础研究进行投资，从而为其研究渠道注入最新概念、技术、基础设施原型，以及民营企业所需的训练有素的工作人员，完成其网络空间安全任务。政府也可以推广技术转让机制，从而加速采用行业内的这些最新技术，部分技术可以通过支持性能指标、模型、数据集和测试台来实现，可以评估最新产品和最佳实践。

为了公益而在社会所有部门中广泛采用的最新知识产生过程中，联邦政府赞助的基础研究是一种独特的国家投资形式。这种研究主要出现在大学和国家实验室。作为营利性实体机构，公司一般会专注于短期效果，或者能够提供近期竞争性优势的专利研究。研究型大学的任务就是从长远角度考虑问题。大学和国家实验室所开展的无保密研究在相关领域培养了训练有素的人才，并带来了附加收益，同时大学毕业生也可以在相关行业、大学和政府部门实现就业。在信息技术领域追求高级学位的大学毕业生会成为新一代的研究领导者；其他的毕业生则通常会参与创业，这在信息技术历史上已经发挥出了关键作用。大学研究也会加速大学毕业新生的教育变革，同时研究人员会快速将最新理念灌输到大学生课程和教科书中去。

基础性研究专注于特别的难题和复杂事物，通常要数年才能解决。如图 3.1 和图 3.2 所示，长期以来，联邦政府在支持信息技术基础研究方面已经发挥出了核心作用。这种研究的成果处于当前许多十亿美元级信息技术行业的核心位置（这些行业可以改变我们的生活、驱动我们的经济发展，也可以提高我们的安全性。基础研究是一种“公益”性的研究）。所以，联邦政府要在这方面发挥作用。联邦政府支持的基础研究、行业支持的应用研究以及行业产品发展之间高度有效的相互作用导致的结果是，今天的美国成为信息技术行业的全球领导者。

今天，因为我们并不知道怎样建模、设计和创造集成具有完整属性（例如相互怀疑或者任何其他基础安全创新）的系统，所以联邦政府需要扩展其网络空间安全研发方面的综合努力。另外，在不断兴起的技术趋势中，我们面临着实质性的最新挑战。例如，我们还不能完全理解内置设备安全分支网络。在此背景下，互相怀疑的原则必须考虑到互连分支网络、信息存储和设备以及给定网络的计算和通信资源的受控访问。在我们现有的软件开发方法中，安全成为一项越来越严苛的要求，只会让当前笨重、缓慢和昂贵的过程变得更为恶化。附加途径并不能应对系统和软件技术中的远景进步需求，不能提供全新的创意方法来解决安全问题。

在本报告的结果和建议中，我们敦促重新考虑军用/情报以及民用网络空间安全研发之间的联邦投资平衡问题。部分原因在于军用和情报领域主要依赖计算系统以及自我批量运行[1]软件的商业网络和商业供应商。只有通过民用网络空间安全方面的基础性研究，我们才

[1] 来自操作伊拉克自由的两个案例阐明了以下事实：①美国军方所使用的 80%以上的宽带都由商业供应商提供；②其所部署的大部分信息技术系统被直接从商业供应商那里装运出去。特里萨-希钦斯，“美国空间武器化：国际安全含义”，2003 年 9 月 29 日。请参考以下网址：http://www.cdi.org/friendlyversion/printversion. cfm? documentID=1745。

能期望应对我国信息技术基础设施的战略性和渗透性弱点。

我们也会强调技术转让的重要性，因为最新的概念不会自动出现在产品上。为了达到这个目的，信息技术供应商必须为他们的产品和服务建立全新的安全功能。但是，供应商回应了用户的需求，只是在最近，大部分用户、公司、政府机构和个人用户才开始关注网络空间安全。如果缺少重大的网络空间安全需求，那么信息技术供应商基本上会选择为消费者愿意购买的功能添加全新的菜单（具有讽刺意味的是，添加最新的功能和复杂性通常会导致引入更多的安全性弱点）。这种远离网络空间安全的市场驱动性偏好就是许多分析师指出的网络空间安全“死亡谷”。研发可能提供关于操作可行性的相关知识和证据，但是如果缺少消费者对安全的需求，那么供应商很难有更强的动力将最新的安全技术纳入其产品中。

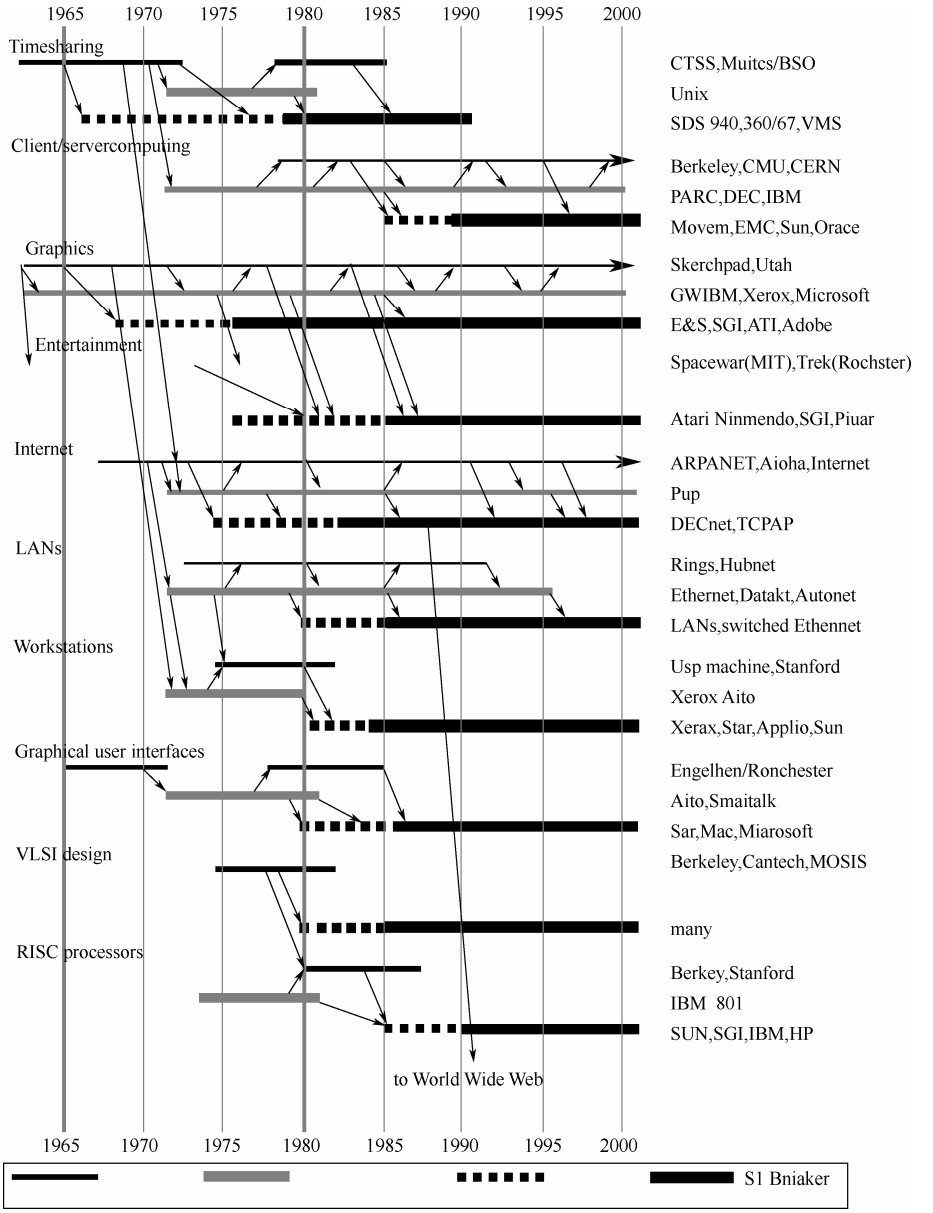

图 3.1　联邦政府支持的基础性研发的历史作用

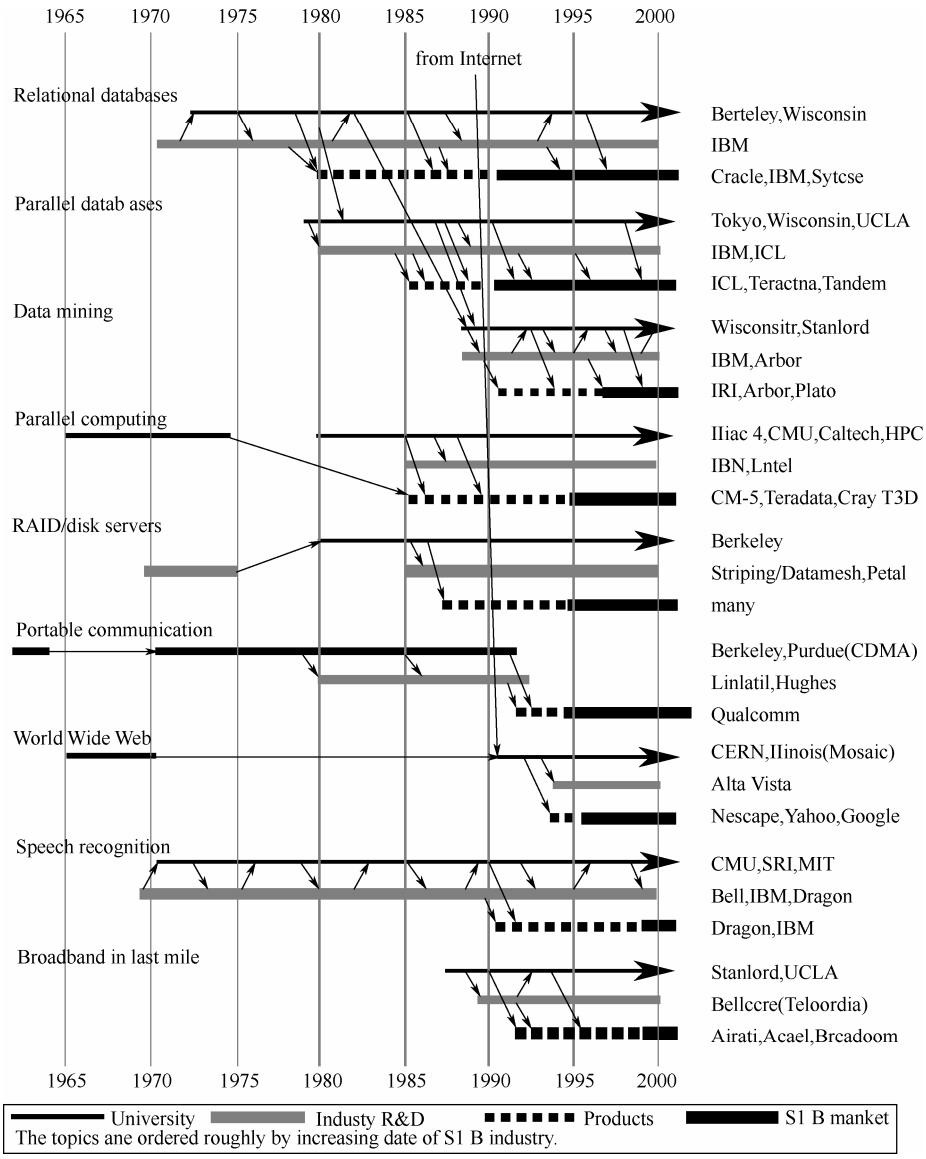

图 3.2　创造数十亿美元的信息技术产业板块

（九）网络空间安全非技术层面注意事项

总统信息技术咨询委员会认为：从能够剔除弱点的技术研发，到能够避免原始弱点的更好设计，只能构成其中一种要素，然而毋庸置疑，其中最为重要的要素就是有效的网络空间安全问题。我们在此粗略指出了亟须社会关注的网络空间安全的几个层面，但是在此报告中并未提出解决方案。

国内外法律的实施。使用连接互联网计算机的敌方，在数千英里外就可以攻击美国境内连接互联网的计算机，就像在隔壁一样容易。通常而言，我们很难识别这些攻击罪犯，甚至当识别出他们之后，跨国犯罪起诉仍旧是一个问题。

教育。我们需要教育公民：如果打算使用互联网，他们需要继续维护和更新其系统的安

全性，以防止被破坏。例如，防止变成分布式拒绝服务的攻击对象或者“垃圾邮件”的分布对象。我们还需要用最佳实践教育公司和组织机构，以便实现有效的安全管理。例如，现在有些大型组织机构已经出台相关政策：它们权限范围内的所有系统必须满足严苛的安全指导方针。我们可以将自动更新程序发送给内网上的所有计算机和服务器，如果最新系统不符合安全政策，则禁止上线。

信息安全。信息安全指的是采取措施保护或者保存网络信息以及网络本身。因此，它还涉及物理安全性、人员安全性、刑法和调查、经济学和其他问题。这些因素需要纳入网络空间安全从业人员教育课程和支持性法律中，并且还需要研发并获得相关技术。

社会学问题。还有若干涉及网络空间安全的领域，其中可能存在利益冲突和需求；作为网络空间安全的任何全面途径的组成部分，这些矛盾需要得到进一步解决。例如，在努力避免攻击或者追查网络罪犯的过程中，我们有必要了解互联网上数据信息包的来源，但是有人认为这些知情权会和个人隐私权或者匿名权产生矛盾。为了引用其他案例，有些国家或者个人会将其看做过滤数据的必要过程，而其他国家或者个人可能将其看做多余的审查制度。这将涉及伦理、法律和社会问题等，和技术问题一样，这些非技术性的问题甚至会让网络空间安全问题变得更具挑战性。

三、联邦网络空间安全研究和发展：当前重点工作、未来影响

为了对联邦政府在支持网络空间安全研发方面发挥的重要作用开展评估，总统信息技术咨询委员会检查了当前的联邦网络空间安全综合研发情况。正如预期，联邦政府对于网络空间安全研发的支持主要来自美国军方、情报界和民用研发企业。委员会机构投资分析发现：联邦政府历来重视基础性研究，并且无保密研发已经发生了多元演化，将我们长期的物理和经济安全置于危险的境地。

（一）军用和情报机构的网络空间安全研发状况

由于认识到地理分布计算系统之间的潜在通信利益，美国国防部高级研究计划局研发了阿帕网，即今天互联网的雏形。今天，无处不在的军用互连远景已经迅速变成了不可否认的现实。

现在，美国陆海空三军严重依赖于网络信息技术系统，其具有扩大的战场效用以及永久性转型的军用战略。但是，在不同的环境（信任环境）中，这些网络和系统的体系结构才得以界定。今天，心怀不轨的个人、组织机构和政府可能会获得破坏信息技术网络所需的知识和工具。结果，这些系统网络的安全问题就变成军方最为重要的问题。

国防机构的研发预算反映了这种紧迫性。尽管陆海空三军的研究机构已经拥有规模较小且极具价值的网络空间安全计划，但是美国国防部高级研究计划局仍将对美国国防部网络空间安全计划进行最大规模的投资。除了直接支持若干网络空间安全研究活动之外，美国国防部指挥、国防研究和工程办公室还提供相关协调和监督工作。

美国国防部高级研究计划局历来会支出大量预算用于资助非密的长期基础性研究——通常是为期五年以上的活动。

委员会机构投资分析发现：联邦政府历来重视基础性研究，并且无保密研发已经发生了多元演化，将我们长期的物理和经济安全置于危险的境地。

这就使得美国国防部高级研究计划局能够在美国最优秀的研究机构内挑选最有才能的

研究人员，以帮助培养学术团体和行业专家。但是，截至 2004 财务年度，美国国防部高级研究计划局对于网络空间安全研发方面的基础性投资[1]极少（如果有的话）。然而，美国国防部高级研究计划局却更多地依赖美国国家科学基金会支持的研究人员来推动基础性研究，借以研发全新的网络空间安全技术，从而使美国军方受益。此外，作为一种战争工具，网络战争的兴起促使美国国防部高级研究计划局对其更多计划进行加密操作。由此造成的综合结果就是，美国国防部高级研究计划局的工作重点从支持传统的非密长期研发努力整体转向保密的、短期的研发努力。

美国国家安全局（NSA）和美国高级研发活动协会（ARDA）对情报机构内开展的网络空间安全研发计划给予了大力支持。美国国家安全局（NSA）网络空间安全研究（机构将其称为信息保证）得到了其信息保证研究小组（R2）的支持。美国国家安全局（NSA）对于此项工作每年拨款大约 5000 万美元，其中大约 20%直接用于基础性研究。学术性研究仅占其中的 6%（300 万美元），比前些年减少很多。当此研究的大部分内容都不保密时，基本上就变成了短期研究。

由情报体系创建并由美国高级研发活动协会（ARDA）支持的技术研发活动，用于改进这个体系的信息系统和网络。美国高级研发活动协会（ARDA）的网络空间安全研发资金达到了大约 1700 万美元，占到了学术研究支持投入的三分之一，并且大部分都没有进行加密。但是，一旦成熟到能够集成进情报体系工具的水平，美国高级研发活动协会（ARDA）通常会对这种研究的结果进行加密处理。

美国能源部也会凭借其在短期以及/或者军用和情报用途方面的所有工作，在网络空间安全研发方面进行投资。

此项工作主要在国家实验室开展。

（二）联邦政府在民用网络空间安全研究和开发方面的投资

没有致力于军用或者情报方面研发（在本报告中指的是“民用”研究）的机构，在美国信息技术基础设施（包括网络空间安全）的进化过程中发挥着关键作用。这些相关机构包括美国国家科学基金会（NSF）、美国国土安全局（DHS）、美国国家标准与技术研究所（NIST）和美国司法部（DOJ）。

目前，只有美国国家科学基金会（NSF）出台了实质性的联邦民用网络空间安全研究计划，它已经对相关活动支持了数年。大部分的工作都在学术机构开展，并且所有工作都没有进行加密处理。其中许多研究都被看做基础研究，但是总统信息技术咨询委员会已经注意到了较短期活动的微妙变化。

在 2004 财务年度内，机构对于网络空间安全计划活动的总投资已经达到了 7600 万美元，其中用于支持研究性计划的资金大约为 5800 万美元。美国国家科学基金会网络空间研究活动的奠基石是其网络信任计划；此计划在 2004 财务年度内建立，并且同时支持个人网络空间安全研究人员以及学术机构的研究中心。

美国国土安全部在其中发挥着双重作用，包括运行责任（例如保证美国国境、财产、经

[1] 联邦政府提供给总统信息技术咨询委员会的数据显示：在 2004 财务年度内，美国国防部高级研究计划局在网络空间安全方面的投资介于 4000 万美元和 1.5 亿美元之间。

济和关键基础设施的安全）和研发活动。研发努力的主要目的是，通过采用改进现有能力的进化措施以及发展进化的最新能力，对国土面临的威胁进行反制。机构科技董事会的各种复杂任务（网络空间安全研发计划所在的任务）包括以下责任：开发相关技术来抵制大规模杀伤性武器，包括放射性武器、核武器、生化武器等。美国国土安全部大部分十亿美元级规模的科技预算都用于研发抵制这些威胁的技术，以及相关的示范性计划。在 2004 财务年度内，网络空间安全研发计划的拨款只有 1800 万美元。美国国土安全部大部分网络空间安全研发活动都是非密的短期活动（只有大约 150 万美元投资于长期研究），并且和美国国家科学基金会合作资助了其中某些工作。

美国国家标准与技术研究所的任务涉及编制相关措施和标准，其活动在促进技术转让方面发挥着关键作用，并且其在网络空间安全方面的作用专注于这种工作类型。美国国家标准与技术研究所 2004 财务年度内在网络空间安全方面的预算为 970 万美元。在最近批准的 2005 财务年度预算中，美国国家标准与技术研究所计算机安全部对于网络空间安全方面的拨款增长了 1000 万美元。美国国家标准与技术研究所也得到了诸如美国国土安全局等联邦机构的拨款支持，并且和美国国家安全局达成了合作伙伴关系。此研究所历来和行业开展密切合作，已经提高了在学术界的参与程度。美国国家标准与技术研究所开展的网络空间安全研究计划专注于短期计划。

美国司法部下属的国家司法协会已经在打击电子犯罪方面制定了 700 万美元的预算。

（三）军用/情报部门以及民用网络空间之间的关系

1. 军用和情报体系从民用部门投资的研究拨款中获得巨大利益

从历史上来看，军用和情报体系主要通过大力支持美国国防部高级研究计划局和美国国家安全局开展的长期学术研究，从民用部门投资的研究拨款中获得巨大利益。但是，两个机构转向支持短期、保密研究以及随后减少支持民用研究领域，导致此体系实力的折损。因为从传统上而言，许多关于网络空间安全的理念、解决方案和人才都来自民用研究领域，所以民用和军用部门都必然在这种趋势中受损——这是军用和情报机构自身认识到的问题之一。但是，这些机构并没有明显表现出转型其现有的、更为短期的基于任务的途径的趋势；同时，从理论上而言，在支持民用网络空间安全研发领域内的空白可以由其他机构来填补，但是截至目前仍未实现。

作为联邦政府所开展的最为宏大的信息技术计划之一，美国国防部全球信息网（GIG）阐明了减少民用网络空间安全方面的投入所带来的负面影响。为了改善美国的军用通信系统，美国五角大楼计划部署美国国防部全球信息网（GIG），这是一种连接到武器、情报和军事人员以实现“网络强化”战争的多层网络系统。当研发和部署美国国防部全球信息网（GIG）的成本不再是一个公共记录问题时，美国总审计局最近出台的报告预测：它在 2010 年的成本至少要达到 210 亿美元，在此之后[1]，还会增加更多额外支出。

2. 委员会评估披露了有利于保密军用/情报网络空间安全研发以及短期研究的显著变化

美国国防部计划让美国国防部全球信息网（GIG）最为敏感的部分自负盈亏，从而降低

[1] 请参考以下网址：http://www.gao.gov/new.items/d04858.pdf。

暴露在公众信息技术基础设施中有关的潜在军用不安全性。但是，预计美国国防部全球信息网（GIG）中某些敏感度较低的部分会连接到互联网，至少会连接一段时间。当高度敏感的国防网络和民用网络实现交叉时，就会引入弱点，同时使得这两个体系寻求合作，以期改进民用信息技术基础设施的安全性。而且，经济现实表明：今天的军用网络和明天的美国国防部全球信息网（GIG）会使用民用商业硬件和软件，同时将这些网络暴露在这些产品的安全弱点之下。因此，作为未来的一种安全的信息技术基础设施，成功的美国国防部全球信息网（GIG）还在一定程度上依赖于民用信息技术基础设施安全性的改善。因为民用研发体系只能使用无保密研究结果，所以减少对于这种体系的支持，无疑会对未来安全产品和实践赖以发展的基础研究能力产生不利影响。

（四）当前联邦努力评估

委员会对于联邦网络空间安全研发综合努力的评估已经披露出两种令人不安的趋势：第一，有利于保密军用和情报研发的明显变化，使其难以接触到民用部门；第二，与长期基础研究相比，有利于短期研究的军用/情报和民用部门发生的明显变化。这些趋势应当引起决策者的关注，因为它们可能妨碍基础网络空间安全研究的渠道，这对于保障美国信息技术基础设施的安全而言是至关重要的。

如果允许民用领域内的研究停滞不前（如果允许当前趋势继续的话，就有可能发生这种情况），那么我们国家赖以生存的信息技术基础设施就会进一步遭到削弱。因为任何互联系统都可以通过其最薄弱的环节进行攻击，甚至是预计继续连接到民用系统中的美国军用系统，都会成为攻击对象。但是，为网络空间安全研发提供主要支持的机构只有美国国家科学基金会和美国国家标准与技术研究所，美国国土安全局也在一定程度上介入民用领域。其中，美国国家科学基金会为民用网络空间安全方面的基础研究提供了大力支持。

正当所有机构不断警告和强调对于短期研发予以拨款以解决直接的任务要求时，委员会的分析表明：对于长期基础研究的拨款支持（发展领先的优势方案来解决更为复杂的问题的必要的初期形式）已经远远落后。总之，联邦对民用网络空间安全领域基础研究的投资只是网络空间安全研发领域内整体联邦投资的一小部分[1]而已。

总统信息技术咨询委员会认为：联邦政府对于民用网络空间安全基础研究方面的预算必须大大增加，否则，美国的安全和技术优势将会严重受损。下文将提供美国信息技术咨询委员会在解决这些相关问题方面给出的建议。

四、结论和建议

（一）转型期的研发重点

当前，对于美国通信、商业和管理方面涉及的实体性基础设施而言，信息技术（IT）基础设施显得至关重要，但是，它却非常容易受到恐怖分子和罪犯的攻击。通过部署健全的安全产品并贯彻良好的安全实践，民营企业在保障国家的信息技术基础设施安全方面发挥了重

[1] 在通过充实而漫长的努力确定具体的预算数据之后，总统信息技术咨询委员会预计：这个比例介于20%和25%之间。

要作用。但是，通过支持研发能够强化这些产品和实践性能的网络空间安全技术，联邦政府也可以发挥关键作用。美国总统创新技术咨询委员会（PITAC）发现：联邦政府需要从根本上改善这种网络空间安全途径，才能更好地履行这个方面的责任。

结论 1：联邦研发预算并没有为民用网络空间安全基础研究提供充足的拨款资金。

建议 1：美国国家科学基金会（NSF）每年在这个领域内增加 9000 万美元的预算支出。其他机构也应当对于民用网络空间安全基本研究实质性地增加拨款，尤其是美国国防高级研究计划署（DARPA）和美国国土安全局（DHS），应当划拨这些款项，至少要适当地处理“优先考虑的网络空间安全研究”中列出的十个重点领域。根据国家未来的网络空间安全发展态势，拨款可以进一步增加。

讨论：

（1）短期修补陷阱。

今天，大部分民营部门网络空间安全拨款是为了解决直接需要，例如扩张现有的国防体系，在设计低劣或者缺陷系统中安装补丁。这些需要都是合法而重要的预算来源。但是，解决这些需要却类似于填补堤防漏洞。

联邦网络空间安全研发还具有短期重点。若干年后，许多机构预计能够从其最近的网络空间安全研发投资中获益。当前，长期网络空间安全基础研究方面的不足意味着：我们还没有做好应对明天弱点的准备，并且我们正在设计本质上更为安全的未来系统。

2001 年 10 月，美国国家工程协会总裁威廉·A·伍尔夫发表国会声明称：“计算机系统研究人员过去与现在同等重要。我们实际上没有建立安全系统的研究基础……当资金缺乏时，研究人员会变得非常保守，并且对于传统睿智的无畏挑战不可能通过同行审查。结果，渐进主义就会变成规范。”[1]

今天的急迫问题要求我们继续解决直接需要，并开展短期研究。但是，如果不突出重点，我们就无法实现网络空间安全方面的重大进展。在网络空间安全方面的长期基础性研究需要得到实质上的强化，从而为未来的网络空间安全努力提前打好基础。

（2）民用网络空间安全研究的重要性。

民用网络空间安全研发指的是由民用联邦机构、大学、公司和大量人员使用的计算系统、网络和软件所涉及的无保密研发。在民用网络空间安全中研究成果的受益人之一是广大的信息技术市场，其中包括商用互联网、与其连接的网络，以及大部分的私人计算系统。然而，民用研究在国土和国家安全方面发挥的关键作用却并不广为人知。民用网络空间安全基础研究为建立系统打下了基础。这其中包括控制公用基础设施、支持运输和金融部门以及构成军用网络的系统、网络和软件。因此，民用网络空间安全方面的非密研究在美国整个网络空间安全方面发挥着重要而基础性的作用。

通常，民用研究和军用及情报用途的保密研究有着明显不同。当向公众泄露信息可能破坏国家安全（如泄露美国关于敌手实力的情报或者泄露我们的军用信息战斗实力）时，通常会进行保密研究。

因此，我们有充足的理由追求保密研究，但是如果以非保密研究作为代价的话，也就没有优势可言了。例如，保密研究的成果通常不能商业化应用，因为这样做会将其内部运作置

[1] 请参考以下网址：http://www.house.gov/science/hearings/full/oct10/wulf.htm。

于公众监督之下。因此，在很大程度上，保密网络空间安全研究不能用于通用的民用网络空间安全市场，并且它对于商业互联网及其潜在技术或者信息技术基础设施（它们能够加固美国关键基础设施）不会产生广泛影响。相比之下，民用网络空间安全方面的无保密研究通常会使保密系统受益，因为在保密世界中很少会面临根本性的安全问题。

此外，非保密研究拨款能够增加精通网络空间安全的专业人士的数量，而保密网络空间安全研究拨款并非如此，这是本报告中识别的一个关键问题。最终，保密研究的公共政策审查和监督很难达到最佳状态，这就意味着在非密研究方面的拨款支出并没有效率。

（3）研究方向。

正如伍尔夫博士声明中指出的那样，今天我们对于许多涉及网络空间安全的根本性问题还没有找到满意的答案：

当初次部署时，我们怎样建立安全、可靠、复杂的软件集成系统？

在敌对势力入侵或者出现自然灾害时，我们怎样建立能够继续可靠运行的大型分布式系统呢？

我们怎样确认从第三方获取的软件能够正确地执行指定功能，并且只执行此功能呢？

当存储在分布式系统中或者通过网络传输时，我们怎样保证个人身份、信息或者法律交易的隐私权呢？

我们怎样在许多组织机构和地点，建立能够验证大批用户身份的系统？

我们怎样容易地确定互联网传输信息的源头呢？

我们怎样自动确定通过互联网传输的信息是恶意的还是善意的？

委员会分析了 30 多份关于网络空间安全研发的报告，借以分析 10 个拨款支持的重点领域。这些领域都是最重要的领域。如果没有这些领域内研究的重大进步，美国就不能够保障其信息技术基础设施的安全性。有人可能认为这份关于设定拨款重点的列表过于笼统，还有人会发现他们认为关键的漏洞。委员会认为：此份列表在这些观点之间达成了平衡。网络空间安全是一个复杂而多元的问题。这并不是一剂强心针。

（4）联邦网络空间安全研发拨款计划。

由于支持整个科学和工程企业方面的基础研究，美国国家科学基金会成为了民用网络空间安全基础研究方面的主要拨款机构。委员会认为：美国国家科学基金会计算机和信息科学以及工程董事会，尤其是其网络信任计划的网络空间安全研究投资占据了民用网络空间安全基础研究方面大部分的联邦拨款，所以相对于美国的网络空间研究需求而言严重不足。在 2004 财务年度内，网络信任计划收到了 390 份研究提案，并且总计拨款 3100 万美元。这些提案 8%的成功率（6%要求资金）比美国国家科学基金会范围内的数字小三倍。在科学同行评审中，只有 25%的提案被认为值得支持。而且，所支持的大部分提案拨款资金水平都低于所要求的水平。

网络信任计划的经验显示：在高质量研究上可以投入四倍的预算，以便为美国网络空间安全的关键改善打好基础。

从资金额方面来看，美国国家科学基金会可以为民用网络空间安全基础研究增加大约 9000 万美元的预算。

总统信息技术咨询委员会预计 2004 财务年度的预算介于 20%和 25%之间。联邦对于网络空间安全研发的支持主要用于民用网络空间安全基础研究。鉴于民用网络空间安全可以在

美国的整个关键基础设施方面发挥核心作用，委员会认为：应当增加民用研究方面的拨款，这在整个网络空间安全研究预算中占了较大比例。

美国国家科学基金会应当继续成为民用网络空间安全方面的主要拨款机构，委员会建议：美国国家科学基金会不应当成为民用网络空间安全基础研究领域不断投资的重点。不同的机构会为基础性研究提供不同的动机，因此会更广泛地增加将相关研究用于其任务的机会。

委员会认为：美国国防部高级研究计划局和美国国土安全局应当增加其对于民用网络空间安全基础研究方面的支持。不断增加的支持会使得每个机构（美国国防部高级研究计划局过去在这方面拥有经验）和整个国家受益。

总统信息技术咨询委员会建议：美国国家科学基金会计算机科学及工程学部（NSF CISE）对于民用网络空间安全基础研究方面的预算不能以牺牲计算机科学及工程学部的其他部分费用作为代价。计算机科学及工程学部的提案成功率只有 16%（研究拨款为 14%），在美国国家科学基金会范围内平均只有三分之二。如果没有处理好计算机科学及工程学部和其他学部之间的现有差距，那么计算机科学及工程学部的主要拨款资金就会转向网络空间安全，这样会恶化其他计划的紧张局势。而且，在计算机科学及工程学部其他领域内的许多工作都有利于网络空间安全，因此，对这些领域拨款的减少，也会妨碍预期生产目标[1]的实现。最终，某些层次的“失败”联邦计划管理者不必受到惩罚。基础性研究可以在较长的时间框架内开展，并且可以缓和较高的回报风险。如果联邦拨款下发机构的刺激结构鼓励避免失败，那么有利于渐进式工作的研究（允许可能出现明确的预期结果）就会形成规范。但是，许多专家对于网络空间安全研究挑战的评估证实：渐进式工作不可能在某些最为困难的问题上形成解决方案[2]。

结论 2：美国的网络空间安全研究机构太小，不足以支持为美国提供保护的网络空间安全研究和教育计划。

建议 2：联邦政府应当努力在研究性大学招聘和保留网络空间安全研究人员和学生，以期在十年后将民用网络空间安全基本研究机构的规模至少扩大一倍。尤其是联邦政府应当增加对于民用网络空间安全方面的稳定性拨款，并且应当支持相关计划，以使研究人员能够从其他领域转入网络空间安全研究领域。

讨论：

网络空间安全问题已经成为计算机科学和工程研究这个细分板块内的焦点问题。在上文引用的声明中，伍尔夫博士指出：“在美国，只有极少数能够深入思考网络空间安全问题的学术型长期基础研究骨干人员。”委员会同意这种评估结果，并且预计：美国的学术机构所雇佣的活跃网络空间安全或者网络保证专家人数不足 250 人，而且，其中许多专家却缺乏在此领域内正规的培训或者广泛的专业经验。

---

[1] 若干实例：在同时识别出劣势以及先进优势后，理论计算机科学加强了许多加密研究的基础。算法研究帮助确保安全设计协议可以有效地实施。编程语言研究可以帮助解决较高抽象范围内的安全问题，并且可以增加功能，例如软件的安全保证功能。软件工程可以帮助消除通常被利用的软件安全漏洞。并且，最新的计算机体系结构可以在更快和更精细的维度提升保护水平。

[2] 请登录以下网址：http://www.cra.org/grand.challenges，参考计算研究协会的信息安全宏大挑战。

联邦政府应当努力在研究性大学招聘和保留网络空间安全研究人员和学生。

当前领域内较小规模的后果包括：可以对有效调查的所有研究话题进行研究数量的限制，因为在一个主题内生产性的工作通常要求关键的研究人员。在这些较小的研究领域内，研究的支持性基础设施（例如技术会议和定期刊物）也较难发展。最终，领域的较小规模就会使其很难为此专业储备较多的学士和硕士在读生。当美国对于网络空间安全从业人员的需求不断增长时，这种断层确实存在。

建议 1 和建议 2 相辅相成。为了强化并扩大网络空间安全基础性研究体系，联邦政府应当采取以下措施。

提高联邦政府给予网络空间安全基础性研究的拨款。如建议 1 中提到的那样，实质上提高拨款水平对于建立较大的网络空间安全基础研究体系而言是必不可少的。

为网络空间安全基础性研究提供稳定的联邦拨款。稳定的拨款水平（这是一个独立于绝对拨款水平的问题）对于实现这个领域的成长是十分关键的，因为对于进入此领域感兴趣的人员知道：他们可以在此领域拥有未来的发展空间。

支持将研究人员从其他领域转入网络空间安全研究领域的相关计划。尝试改变领域未来的研究人员需要获得拨款以寻求最新的工作成长空间，但是面临着重重困难，因为他们在这个全新的领域内还没有任何档案记录。公休和类似计划可以使潜在的网络空间安全研究人员获得经验和知识，因此能够使他们更快地对这个领域作出贡献。

着重非密网络空间安全研究。美国大部分学术研究人员无须经过忠诚度调查，就能开展保密工作。而且，许多研究型大学认为保密研究和有利于整个社会[1]的知识生产者发挥的作用之间存在矛盾。网络空间安全不断增加的保密趋势已经对大学网络空间安全基础性研究人员产生了负面影响。

培养一个较大规模、更为强大的网络空间安全基础研究领域，将会帮助确保生成革命性的全新理念（和渐进式发展相反）。委员会认为：再过十年，网络空间安全基础性研究领域的规模翻一番是很有可能的，并且可以帮助推动美国网络空间安全的研发努力。

结论 3：当前的网络空间安全技术转让努力并不能够成功地将联邦研究投资转化为民用领域内的最佳实践和产品。

建议 3：联邦政府应当加强网络空间安全技术转让合伙企业和民营企业之间的合作。尤其是联邦政府应当重点推动各种指标、模型、数据库和测试平台的研发，以便对全新的产品和最佳实践进行评估；民营企业应当在展示全新网络空间安全成果的年度跨界会议上给予联合赞助；对于拥有前瞻性研发理念或者技术的研究人员的技术转让努力（与产业合作）给予拨款支持；鼓励联邦政府支持作为研究人员、实习生或者顾问的研究生和博士生获得行业经验。

讨论：

技术转让可以使联邦政府支持的研发成果融入通用产品中去。长期以来，联邦政府资助的信息技术研发成果成功地融入了民营企业中广泛采用的产品和最佳实践中。图 3.1 突出强调了催生数十亿美元全新产业的、联邦政府资助的信息技术基础性研究的 19 个案例。这就

[1] 当联邦政府对于外国毕业生可以开展的工作以及他们学习的课程进行限制时，就会产生类似的问题，因为毕业生是大学研究计划的有生力量。

证明：当学术机构和政府密切合作时，这种协作是有可能实现的。

联邦政府资助的信息技术研发同时扩散到产品和实践中去，这样既有利于消费者，也有利于开发商。

消费者的受益来源包括：便捷使用的更快的硬件、更快的网络、更好的软件，以及更为频繁的时间和人力节约升级。

信息技术研究通常会生成全新的理念和原型[1]，可以被快速开发成全新或者改进型的商业产品。这些创新产品的开发商可以自由选择是否将这些创新理念引入市场，以便让所有消费者获益。

和其他信息技术产品有所不同，网络空间安全收益可以通过信息技术系统是否存在问题来衡量。因为这些收益市场历来较小，所以在创业型公司和大型公司中利润有限。

委员会认为：鉴于技术转让的价值和难度，联邦政府应当支持相关计划，以便将现有和未来的网络空间安全研究成果融入商业产品或者最佳运营实践中去。联邦政府应当采取以下措施。

加强开发相关指标、模型、数据库和测试台，以便对全新产品和最佳实践进行评估。

和民营企业联合赞助年度跨界会议，从而展示全新的网络空间安全研发成果，尤其是联邦政府开展或者赞助的研究。[2]

要求批准提案，以描述其研究成果的潜在实际效用，使得建议 4 中指定的协调机构搜集和出版这些描述。当进行基础性研究时，通常没有预见的任何直接过渡渠道，网络空间安全研究通常要在身份识别问题背景下开展，并且我们还需要备案和真实世界问题之间的逻辑联系。

成立拨款基金，用以支持已经开展远景理念或者技术的研究人员的技术转让努力。这种基金还可以帮助研究人员寻求产业合作，从而将产品或者改进设计快速引入市场。

建立并维护联邦资助的网络空间安全研究的国家数据库成果，允许供应商识别可以融入商业产品的理念。

鼓励联邦政府支持的研究生和博士后获得和研究人员、实习生或者顾问一样的行业经验。

通过联邦政府的小型企业创新研究（SBIR）计划和小型企业技术转让（SBTT）计划，鼓励机构投资于网络空间安全研发成果的技术转让。

通过密切合作，联邦政府和民营企业可以将联邦资助的网络空间安全研究成果有效地转化为商业产品，并建立创新型的网络空间安全劳动力，这样做可以帮助我们的社会认识到这些研究带来的潜在收益。

结论 4：由于协调和监管不佳，导致当前联邦政府的整个网络空间安全研发努力重点不突出。

---

[1] 请参考 1994 年美国国家研究委员会计算机科学和电信委员会“实验计算机科学家和工程师学术生涯”。

[2] 在 2001 年之前，美国国家标准与技术研究所和美国国家安全局赞助的年度国家信息系统安全会议履行了这些职能。这是大部分安全专业人士参加的活动。会议议程为邀请特别演讲者、颁发美国国家信息系统安全奖项（通常被认为是此领域内的最高奖项）以及供应商和计划奖项，还有展览当前先进技术的大型供应商展览会。

建议 4：关键信息基础设施保护署（CIIP）跨界工作组应当重点负责协调联邦网络空间安全研发努力。在网络和信息技术研发计划中，应当强化和融合这种工作组的职责。

讨论：

在联邦政府内，设置了若干协调机构，其涉及领域包括各种层面的网络空间安全研发。具体包括：美国国家科学技术委员会（NSTC）下属的关键信息基础设施保护跨界工作组（IWG/CIIP）；美国国家科学技术委员会（NSTC）下属的、负责协调网络和信息技术研发计划的网络和信息技术研发小组委员会，以及小组委员会的协调组，尤其是高信任软件和系统协调小组[1]、大规模网络协调小组[2]、信息安全研究委员会（IRC）。

这些协调机构会定期召开会议（通常为月度例会），为机构代表提供共享信息的机会，赞助跨界研讨会，促进联合或者协调资助相关计划和研究，并且作为学术专家和行业代表提供输入数据的一种手段。

然而，作为关键元素，政府在机构网络空间安全研究计划和议程之间进行的有效协调，却在很大程度上出现了缺失。委员会认为：关键信息基础设施保护跨界工作组已经进行了跨界努力，从而优先处理网络空间安全研究领域，其目的是为跨界网络空间安全研发计划编制联邦议程，并且着重围绕最为优先考虑的需求。这种初步工作受到了鼓励，并且对于联邦投资在网络空间安全研发计划中的效率而言是至关重要的，因为如果缺少这些协调活动，机构就会围绕其自身任务开展工作，而非整个联邦政府优先考虑的研发重点。另外，随着网络空间安全研发计划拨款额度的不断增长，我们需要更大范围的协调努力，从而确保做出理性的决定。

因此，关键信息基础设施保护跨界工作组在协调联邦政府网络空间安全研发计划中发挥的作用有待进一步强化，并且应当融入网络和信息技术研发计划中去。

通过强化协调可以实现的目标如下。

协调联邦机构之间的研究议程，使得最为重要的议题能够变成重点任务，避免重复努力，并在必要时适当鼓励联合支持的工作。

完善联邦政府和民营企业之间的交流和沟通。关于联邦网络空间安全研发投资的有效决策，要求政府更好地理解民营企业研发活动和趋势以及民营企业的运营状态。

召集政府、大学和行业范围内的相关人士参加研讨会，以便就高级战略和问题（例如长期体系结构设计问题）交流信息，从而应对不断增长的网络空间安全挑战。如果没有这些研讨会，针对主要供应商的竞争性和反垄断限制要求，就会让对话变得很难继续。

通过联邦政府，系统性地采集关于网络空间安全研发活动的数据。获取总统信息技术咨询委员会审批的网络空间安全预算数据。跟踪网络空间安全研发计划的进度，在预算讨论过程中实现更高的透明度，必须及时提供精确的最新数据。

跟踪网络空间安全研发计划的学术进度及其对于网络空间安全数据获取的影响，并在联邦政府范围内加以使用。关键信息基础设施保护跨界工作组应当就联邦网络空间安全研发投资的整体效果定期出台报告。

关键信息基础设施保护跨界工作组协调的网络空间安全研发计划，应当引入网络信息技

[1] 请参考以下网址：http://www.nitrd.gov/iwg/hcss.html。

[2] 请参考以下网址：http://www.nitrd.gov/iwg/lsn.html。

术研发计划中去，关键信息基础设施保护跨界工作组不仅应当向其当前总部机构以及美国国家科学技术委员会（NSTC）下属的小组委员会报告，而且应当向网络和信息技术研发小组委员会报告。我们需要将网络空间安全需求的进展完全融入信息技术系统中去，这就要求网络空间安全研发计划变成整个信息技术研发计划不可或缺的组成部分。在网络和信息技术研发小组委员会的领导下，通过引入关键信息基础设施保护跨界工作组就能够实现这一点。信息安全研究委员会（IRC）应当继续和其他的联邦网络空间安全研发机构开展密切合作和协调。

（二）网络空间安全研究重点

通过对30多份网络空间研发报告的分析，委员会确认了亟须不断关注的10个重点领域。这些领域都极其重要。如果没有这些领域内的重大进步，美国就不能确保其信息技术基础设施的安全性。下列领域为随机排序，并不代表其重要性等级。

1. 认证技术

为了达到不同的目的，需要对诸如硬件、软件、数据和用户等指标进行认证，其中包括识别、授权和完整性检查等。这些指标必须确保安全、容易验证，支持数十亿级元件的应用，并且可以实现快速执行。传统密码系统方法已经在关注安全性，但是还不能在相关环境中实现有效应用。例如，每秒数百万数据包必须由单一网络路由器进行认证。许多有用的工作已经在密码协议中实现。二级研发主题如下：

- 为大规模公众关键分配和管理以及其他可能的途径研发基础设施和协议；
- 认证和废止管理；
- 集成生物测定和物理代号；
- 从识别程序中退耦认证，以解决隐私问题。

2. 安全基础协议

只有为数不多的管理互联网运行的协议具有足够的安全性。例如，为了将流量指向错误的交替网址，攻击者可以很容易地欺骗（或者“戏弄”）诸如边界网关协议（BGP）（当通过互联网时，它控制着数据包经由的路径）等协议，以及诸如域名系统（DNS）（它控制着数据包的目的地）等服务。这些攻击者可以拦截、监控、篡改或者操纵互联网流量，通常无法追查和检测。如果想让互联网变成可靠的通信媒体，我们必须开发能够应对诸如拒绝服务、变体和哄骗等威胁的基本协议安全版本。而且，我们需要保护基本协议免遭寻求协议自身弱点的瘫痪式攻击。二级研发主题如下：

- 互联网协议电话（VoIP）、无线网络以及虚拟专用网络（VPN）安全性，其中每个协议都比互联网基本协议更为复杂，并且任何一个协议都没有实现充分的安全性；
- 即使在与不信任方共享和执行协议时，仍旧要保障协议的安全性；
- 权衡安全和性能。

3. 安全的软件工程和软件保证

今天，我们的商业软件工程缺少科学的基础结构和严格的控制流程，因此很难以可接受的成本生产出高质量的安全产品。常用的软件工程实践允许诸如不当处理缓冲溢出等危险错

误的存在，这就使得数百攻击计划有机可乘，每年都会破坏数百万台计算机。将来，当国内外的敌对势力越来越擅长将恶意代码插入关键软件时，美国可能会面对更具挑战性的问题。从避免基本编程错误，到发展保证安全的大规模系统，甚至当部分系统软件遭到破坏时，我们亟须研发全新的安全软件工程项目。二级研发主题如下：

- 囊括基础安全性能的编程语言和系统；
- 当在不同的环境中部署时，仍旧保持安全性的便携式或者可重复使用的代码；
- 获取应对安全问题的明确标准和设计规范的技术；
- 检验和确认相关技术，从而确保已经执行了备案要求和技术规范；
- 对比模型和指标，从而确保已经满足指定标准，并能够对备选方案实施评估；
- 有效而经济地验证技术，验证计算机代码并不包括备案或者要求的可利用性能。

4. 整体系统安全性

在诸如互联网及其节点等复杂、多层和全球化基础设施中实现有效的安全性，要求的不仅仅是其构成元件的安全性。建立和完善认证方法、基本网络运行安全协议并改善软件工程，显然成为解决这个问题的不断进化的方案。但是，最为重要的是，研究人员必须从一开始就要确认：端到端的构建方法以及整体的安全性都必须超过单个元件的安全性。

例如，消费者认为他们基于加密套接字协议层的在线银行交易确实安全。但是，通过哄骗相关的潜在协议或者终端用户软件，敌方仍旧可以让用户的交易看起来受到了加密套接字协议层的保护，同时实现盗窃机密数据。它还有可能破坏终端计算系统的安全性，甚至在安全传输时获得相关数据。

软件适用性本身是网络空间安全方面一个合法而重要的研究主题。误用的软件、敌对或者混乱的用户界面会导致用户失败和未经授权的工作区，甚至可以破坏大部分健全的安全系统。我们需要研究怎样制作大型复杂系统，从而使得软件以意外方式开展互动，保护整个系统的安全。最终，基础研究应当解决全新的整体安全体系结构的发展问题，包括硬件、操作系统、网络和应用程序。二级研发主题如下：

- 通过信任和非信任元件可以建立安全系统，在全新系统中集成遗产元件；
- 主动减少弱点；
- 保障敌方联合操作以及/或者联合拥有的系统的安全性；
- 全面解决不断增长的内部人员威胁的问题；
- 在复杂系统中建模和分析应急失败；
- 人因工程，例如推广用户重要性意识和安全的界面；
- 通过改进安全性，支持保护隐私。

5. 监控和检测

无论以前研究领域内取得了多少进步，仍旧会出现不可预料的事件。当出现这种情况的时候，我们需要监控和理解运行状态的工具，以便适当地部署配套的防卫措施。用于监控反常网络活动并快速识别潜在深层次原因的工具还非常原始。当敌对势力掌握越来越多的知识，并且互联网变得更广泛和更复杂时，敌对势力所利用的当前优势会逐渐成长。

二级研发主题如下：

- 当通过增加监控性活动来检测可能的攻击时，进行动态互动保护；

- 全球范围内的监控和入侵检测；
- 监控系统，以确保它们能够满足指定的安全政策；
- 基于改进模型的更好工具能够表现出“规范”的行为；
- 在出现危机时，进行实时数据采集、存储、处理和分析；
- 允许操作者更好地理解事件进程的可用表现界面。

6. 缓解和恢复方法

我们必须设计安全系统，以便对于无法预料的事件和攻击做出快速响应，并从随后的破坏中恢复过来，这是大型化、复杂化互联网及其节点系统尤其要面临的挑战性任务。在其他异常复杂的系统中已经处理了这种问题，例如，航天飞机，其中已经做出实质性投资来实现最大化的可靠性和冗余度。在开发配套方案来制造可靠的互联网和关键计算机系统以应对攻击方面，我们做的努力还不够。二级研发主题如下：

- 在停运和攻击之后，快速、自动恢复监控数据；
- 能够从停运和攻击中快速恢复的全新系统结构；
- 简化系统，从而提高自动化运行的作用，以便减少人工操作者的错误和内部人员攻击，当更新软件和配置时更是如此；
- 故障限度和功能退化。

7. 网络空间法证：捕获犯罪分子和打击犯罪活动

快速逮捕和定罪犯罪分子是执法的主要目标，也是一种威慑。当潜在的犯罪分子认为被逮捕和定罪的概率较大时，他们就不愿意去犯罪。

我们当前调查网络犯罪、甄别犯罪分子、采集和提供证据以及定罪的能力非常有限。问题变得越来越严重，我们却不知道怎样打击网络犯罪。今天，我们只是逮捕了为数不多的网络犯罪分子。

我们亟须研发最新的工具和技术来调查网络犯罪活动并起诉犯罪分子。我们还需要强大的网络空间法证手段，从而证明我们有能力承担法庭举证的责任（包括起诉犯罪分子或者使无辜者免罪）。二级研发主题如下：

- 识别网络攻击的来源，包括跟踪网络流量；
- 基于行为识别攻击者；
- 在不愿配合的网络环境中收集证据；
- 跟踪不断增长的欺诈、身份盗窃和知识产权盗窃流量中使用的盗窃信息，包括从不稳定和不完全清除计算媒体、磁盘、手机、掌上电脑和内置系统中恢复跟踪证据的工具和协议；
- 当数据存储在用时，用于搜索特定信息和指标的大量数据存储工具和协议；
- 开展基础性研究，以便开发发生事故时用于法律调查的法证系统体系结构。

8. 为最新技术建模和建立实验平台

快速开发全新网络安全产品的障碍之一是缺乏在真实世界环境中测试最新技术的现实模型和实验平台。我们已经开展了互联网建模方面的研究，但是仍旧处于初步发展阶段，对于实践的影响还很小。由于互联网规模巨大、复杂性较强，所以这个问题极具挑战性。此外，

互联网工作的现有数据是有限的，并且通常保密。最近我们已经建立了若干联邦计划，但是如果要让可用模型和实验平台变成现实，我们还需要更强更多的研发努力。二级研发主题如下：

- 系统模拟环境；
- 验证数百万节点所涉及的模拟活动；
- 采集并整合大量的数据；
- 设计实验平台，以便为数据保密。

9. 指标、基准和最佳实践

有些科学领域已经建立了广泛认可的指标和基准，以便帮助评估全新技术或者产品。但是，围绕开发网络空间安全的指标、基准和最佳实践方面的研究还相对较少。如果确实存在基准或者认证标准，它们通常已经过时且造价昂贵，甚至有碍于改进安全性。如果没有广泛认可的网络空间安全指标，那么我们就很难将前瞻性开发和陷入僵局的途径区分开来。反过来，当将这些技术融入产品周期时，这样做也会大大增加成本，并且延迟上市时间。二级研发主题如下：

- 开发安全性指标和基准数据；
- 经济影响评估和风险分析，包括客观的风险措施、缓解风险和防卫成本；
- 用于评估合规性以及/或者风险的自动化工具；
- 用于评估弱点的工具，包括源代码扫描；
- 发现和备案最佳实践，包括审计程序、配置和补丁管理。

10. 可以破坏网络空间安全的非技术性问题

众多的非技术性因素（包括心理因素、社会因素、制度因素、法律因素和经济因素等）可以通过网络和软件工程不能单独应对的途径来破坏网络空间安全性。我们需要超出技术范围并延伸到其他领域的网络空间研究项目。我们可以通过信息技术基础设施人为和组织机构方面的研究来寻求人的行为因素中的解决方案。二级研发主题如下：

- 开展相关战略，以改变对于个人和公司而言造价昂贵的较大规模网络安全的广泛固有观念（这种观念会妨碍此领域内的软件开发）；
- 通过风险管理和风险分析，寻求相关途径来强化信息技术基础设施中隐私保护和信任的现有价值；
- 围绕伦理、文化、行为以及可以导致非技术性安全失效的其他因素，检验人们怎样和信息技术基础设施展开互动；
- 对于导致人们实施网络犯罪的社会学和行为学现象开展研究；
- 考虑国际法律和标准，以及其对于网络空间安全技术、政策和实施方面产生的影响；
- 网络驱动的商业参与，包括相关税务领域和付款方面的司法纠纷，寻求相关途径解决网络空间安全和网络软件方面的这些问题；
- 在美国境外开发和转让网络空间安全技术时产生的国家和商业安全问题。

网络空间政策评估

一、前言

网络空间几乎涉及每个人和每件事。网络空间提供了一个创新与繁荣的平台，提供了全世界改善整体福利的方法与途径。但是由于很多人都可以轻而易举地触及管控松散的数字基础设施，各种巨大的风险正在对国家、民营企业和个人权利构成威胁。美国政府有责任解决这些网络空间的战略缺陷及弱点，确保美国及其公民与世界更多的国家共同充分发挥潜力，实现信息技术革命。

主要以国际互联网为基础的国家数字基础设施架构并不具有安全性，或者说韧性比较差。如果这些系统在安全上没有取得重大进展，或在如何构建和运营上没有实现重大改观，则很难让人相信美国能够保护自己免受网络犯罪日益严重的威胁，免遭由国家支持的入侵和军事行动的日益严重威胁。我们的数字基础设施早已经遭受入侵，犯罪分子已经窃取了亿万美元，一些国家和机构团体盗取了知识产权和敏感的军事情报。还有的入侵可能会损坏我们部分关键基础设施。美国的经济和安全利益都是以信息系统为基础的，这些形形色色的风险有可能会动摇国家对信息系统的信赖。联邦政府还没有组织起来有效地解决这个目前或在未来日益严重的问题。联邦政府很多部门和机构都担负有网络安全的责任，但存在职权重叠的问题，没有一个部门拥有足够的决策权来指挥行动，协调一致地去处理相互矛盾的问题。政府需要综合考虑各方竞争的利益，制定出一个全面设想和计划，以解决美国面临的网络安全问题。国家需要制定出必要的政策和程序，培养相关人才和发展相关技术，以降低网络安全所面临的风险。

无论是在美国国内还是在国际上，信息和通信网络基本上是归民营部门所有并经营的。因此，解决网络安全问题需要建立起政府和民营部门之间的伙伴关系，要进行国际合作并制定国际准则。美国需要拥有一个全面的架构，以确保政府、民营部门和我们的盟国在发生重大网络事件或威胁时，协调一致地做出反应和进行防御。

美国需要开展一次全国性的网络安全讨论，从而使更多的民众认识到网络威胁与网络风险，以确保拥有一套完整的办法来满足国家对网络安全的需要，并履行国家做出的承诺，维护受宪法和法律保护的公民个人隐私权和自由权。

确保信息和通信基础设施安全并具有较强的韧性，仅仅依靠研究新的办法是远远不够的。政府需要加大研究经费投入，这将有助于解决网络安全上存在的弱点，同时也能满足我们经济和国家安全的需要。

二、概述

美国总统指示要在 60 天内完成一份全面、全新的评估报告，对美国网络安全政策和组织结构进行评估。网络安全政策包括网络空间安全和网络空间运行的战略、方针及标准，涵盖了所有的降低威胁、减少弱点、实施威慑、国际参与、应急反应、确保韧性及恢复能力的

政策与行动，并包括计算机网络运行、信息安全保障、执法、外交、军事和情报工作等。这些要素与全球信息和通信基础设施的安全与稳定息息相关。评估报告研究的内容并不包括与国家安全或基础设施安全无关的其他信息与通信政策。由政府网络安全专家组成的评估小组负责汇总产业界、学术界、公民自由与隐私维权团体、州政府、国际合作伙伴，以及国家立法和行政部门提出的具有广泛代表性的意见和建议。本报告对评估小组的结论进行了综述，并概括地说明了在未来如何开始实现拥有可靠、有韧性和值得信赖的数字基础设施。

美国正处在十字路口。全球互连的数字信息与通信基础设施被称为“网络空间”。现代社会的方方面面几乎都离不开网络空间。网络空间为美国经济、民用基础设施、公共安全和国家安全提供了重要的支撑。这项技术已经使全球经济发生了改变，使人们以难以想象的方式联系在一起。然而，网络安全的风险也构成了 21 世纪最严峻的经济挑战和国家安全挑战。数字基础设施架构的构筑更多的是基于互通性和效率上的考虑，而不是从安全的角度进行考量的。因此，越来越多的国家和非国家行为体开始破坏、盗窃、篡改或毁坏信息，这会给美国的系统造成重大破坏。与此同时，传统的电信和互联网日益融为一体，而在其他基础设施领域，互联网正日益成为互联互通的主要手段。美国正面临着双重挑战，既要维护促进高效、创新、经济繁荣和自由贸易的良好环境，又要确保安全、保密，维护公民自由和隐私权。解决网络空间存在的战略漏洞，并确保美国和世界充分发挥潜能实现信息技术革命，这是美国政府的一个基本责任。

再也不能容忍目前的状况。美国必须向世界表明，美国将凭借强有力的领导和对远景的规划，严肃认真地迎接这一挑战。顶层领导应该得到加强，白宫应成为网络安全领导核心，提供指导，协调行动，并取得成效。此外，要落实联邦政府网络安全的领导责任制。这种方法要求明确联邦政府各部门和机构的网络安全任务和职责，同时提供相关政策、法律程序和必要的协调，使各部门能够各司其职。在过去的两年中，我们已经开始实施重大的计划，并通过对各机构的不同任务进行“衔接”而取得了长足的进步，但这样做并没有提供一个完备的解决办法。此外，这一问题超越了各个政府部门和机构的管辖范围。尽管每个部门和机构在网络安全方面都发挥着不可替代的作用，但任何一个部门都不具备足够广阔的视野或足够的权威，来彻底解决这个问题。

立即启动全国网络安全大讨论。美国政府应该与业界共同向民众解释清楚这个挑战的性质，并详细说明国家将通过何种方式来解决面临的问题。从某种程度上讲，也就是让美国公民充分认识采取行动的必要性。人们若不先了解网络问题的危急程度就不可能重视网络安全。因此，联邦政府应借鉴以往成功的宣传经验，发起一个全国性的网络空间安全公众意识教育运动。此外，与 1957 年 10 月苏联发射第一颗人造地球卫星后的一段时间类似，我们正面临一场全球数学和科学技能竞赛。我们继续拥有世界上最好的信息技术产业环境，但同时国家应培养参加全球竞争并保持领导地位所必需的劳动大军。

孤军奋战不可能保证网络空间安全。美国政府应加强与民营部门的合作。政府部门与民营部门的利益是交织在一起的，它们的共同责任就是确保拥有安全、可靠的基础设施。联邦政府在很多方面是可以与民营部门合作的。政府应该探究和开发那些可供选择的办法。政府与民营部门网络安全的合作伙伴关系必须得以发展，并清晰地界定这种关系的性质，包括明确各自的分工和职责。联邦政府应审查现有的政府与民营企业的合作伙伴关系，确定优先任务，采取具体行动，以发挥最大的效能。

美国还需要制定一个网络安全战略，以塑造国际环境，使志同道合的国家就领土管辖权、主权责任与动用军队的相关技术标准和公认法律规范等一系列问题达成共识。国际规范对于建立安全和繁荣的数字基础设施是至关重要的。此外，各个国家和地区不同的法律规定和做法也给创造安全、保密和值得信赖的网络环境带来严重挑战。这些法律上的差异对实现安全、可靠和有韧性的数字环境构成了挑战，并涉及网络犯罪调查与起诉、数据保存、数据保护和数据隐私权、网络防御和应对网络攻击的反应等一系列问题。只有通过与国际合作伙伴的共同努力，美国才有可能更好地应对这些挑战，加强网络安全，并全面享用数字时代带来的巨大利益。

在保护国家免遭网络事件或事故冲击方面，联邦政府既不能全部包办，也不能回避职责。联邦政府担负有保卫国家的责任，各级政府担负着确保公民安全和福祉的责任。但是，民营部门设计、建造、拥有并经营着大部分的数字基础设施，为政府和私人使用者提供网络支持。美国需要有一个全面的框架方案，以确保遇有重大事件发生时，联邦、州、地方和原住民保留地政府，以及民营部门和国际盟友做出协调一致的反应。执行本框架方案需要制定报告制度、针对不同情况的应急计划和灾后恢复计划，以及完成这些计划所必需的协调、信息共享和事件报告机制。

政府与重要的利益攸关方应共同努力，设计一个有效的机制以实现真正共同运作的构想，将政府和民营部门的信息整合成一体，并以此作为信息通畅、按轻重缓急顺序推进减灾工作和做出应急反应决策的基础。

与民营部门合作要求明确下一代基础设施的性能和安全目标。美国应充分利用技术优势满足国家经济和安全需要。即使面对敌人利用先进技术实施的攻击，联邦政府制定的政策也应该能够保证国家安全、知识产权保护和基础设施的不间断工作。联邦政府必须与民营部门及学术界合作，阐明协调一致的国家信息和通信基础设施的性能和安全目标。应与州、地方政府通力合作，制定有效的采购战略，推动市场制造更安全的产品并为公众提供各种有效的服务。政府还应探索另外一些激励机制，包括调整法律责任（安全改善后责任减少，安全条件差则导致责任增加）、补偿及税收优惠，以及新的监管规定和执行机制等。

白宫必须指明前进的道路。在过去 15 年里，美国采取的网络安全措施没能跟上威胁的发展变化。我们需要向国内外证明，美国是在认真地对待网络安全相关的问题、政策和活动。这就要求由白宫挂帅，充分利用整个国家的力量，做到集思广益。

三、导言

（一）什么是网络空间

第 54 号国家安全总统令暨第 23 号国土安全总统令将网络空间定义为信息技术基础设施相互依存的网络，包括互联网、电信网、计算机系统以及重要产业中的处理器和控制器。常见的用法还指信息虚拟环境以及人与人之间的互动。

全球相互连接的数字信息和通信基础设施被称为“网络空间”。它几乎成为现代社会各领域的基础，并为美国经济、民用基础设施、公共安全和国家安全提供重要的支撑。信息技术已经改变了全球的经济，并超乎想象地把人和市场连接在一起。为充分享用数字革命带来的好处，所有用户必须树立起坚定的信心，确信敏感信息是安全的，商业活动不会受到损害，

基础设施不会遭到入侵。世界各国还需要树立信心，相信支持其国家安全和经济繁荣的网络是安全的、有韧性的。拥有可靠的通信与信息基础设施将会确保美国充分发挥信息技术革命的潜力。第 44 届总统网络安全委员会在 2008 年 12 月的报告中明确指出，“美国网络安全保护不力是新一届美国政府所面临的最紧迫的国家安全问题之一。”

保护网络空间需要具有卓越的先见之明和强有力的领导，需要在政策、技术、教育乃至法律等方面进行变革。政府最高领导层、产业界和民间社会共同致力于网络安全，这会使美国在加强国家安全和促进全球经济的同时，继续在创新和尖端技术运用方面保持领先地位。

（二）评估的理由

网络威胁对 21 世纪美国和我们盟友的经济和国家安全构成了最严重的挑战。

越来越多的国家和非国家行为者，如恐怖分子和国际犯罪集团，开始把攻击目标对准美国的公民、商业、重要的基础设施和政府。他们有能力危害、窃取、篡改或完全毁坏信息。持续非法利用信息网络和破坏敏感数据等行为，特别是由国家实施的破坏行动，使美国经济竞争力和军事技术优势蒙受损失。正如国家情报总监最近在国会作证时所陈述的那样，“信息系统、互联网和其他基础设施之间越来越多地连接在一起，为攻击者破坏电信、电力、能源管道、炼油厂、金融网和其他关键基础设施创造了机会。”情报界分析认为，一些国家早已拥有了实施这种攻击的技术能力。

日趋复杂、广泛的犯罪活动，以及网络事件所造成的危害凸显出网络空间恶意行为的危害性，包括损害美国的竞争力、降低对隐私和公民自由的有效防护、破坏国家的安全或使公众失去信任感，甚至瘫痪社会。例如：

- 关键基础设施失灵。根据中央情报局报告，针对信息技术系统进行的恶意活动，已经使海外多个地区的供电设施遭到破坏。在其中的一起案例中，恶意行为曾导致多个城市断电。
- 恶意利用全球金融服务。据媒体报道，2008 年 11 月，一家国际银行付款处理器遭到恶意侵犯，导致遍布 49 个城市的 130 多台自动取款机非正常交易达半小时之久。在媒体报道的另一起案件中，一家美国零售商在 2007 年遭遇了数据被破坏和个人身份识别信息丢失的恶性事件，殃及 4500 万张信用卡和借记卡。
- 美国经济遭受全面损失。业界估计，知识产权与数据失窃在 2008 年给美国造成了高达 1 万亿美元的损失。

本报告中提及的网络安全政策，包括了网络空间安全和网络运营战略、政策和标准，并涵盖了全面降低威胁、减少弱点、实施威慑、国际参与、应急反应、确保韧性和恢复能力的政策及行动；还包括与全球信息与通信基础设施的安全与稳定息息相关的计算机网络运行、信息安全保障、执法、外交、军事和情报活动，但并不包括与国家安全及基础设施安全无关的其他信息与通信政策。

（三）全新的评估

因为认识到所面临的挑战与机遇，美国总统将网络安全确定为本届政府的优先议题，并指示对此进行 60 天的全面审查，以评估美国网络安全政策与结构。评估与信息和通信基础设施有关的所有任务和活动，包括计算机网络防御、执法调查、军事与情报活动，以及与之

有关的信息安全、反间谍、反恐、电信政策和综合的关键基础设施保护等方面内容。由政府网络安全专家组成的评估小组彻查了相关的总统政策令、行政命令、国家战略和政府顾问委员会及民营部门提供的研究报告。评估小组还向政府部门和机构征求了意见，让他们按要求就各自与网络安全相关的特别活动、权限和能力提供材料，并要求政府部门和机构确认那些可能未被列入评估初稿之中的新的需求或已存在的需求。于是很多的法律问题浮出水面，如集中管理问题，政府使用什么样的机构来保护私有重要基础设施，互联网监控软件的安装，自动攻击检测和预警的应用，联邦政府与第三方数据共享和私人信息的保护责任等。评估小组还与联邦政府内外广大利益攸关方进行了沟通。小组力争透明，与产业界、学术界、公民自由与隐私社团、州政府、国际合作伙伴以及立法和行政部门广泛沟通，分析与评估其他相关的计划和事务。面对各方——学术界、产业界和政府——一道努力建立值得信赖和富有韧性的通信与信息基础设施的难得机会，评估小组给这些利益攸关方规定了评估的范围，并要求它们就相关领域提供材料。这种沟通工作包括 40 多次会议，形成了 100 多份带有具体建议和目标的文件。相关各方的反馈和公开说明，如国会证词等有助于确定重大需求，指明政策差距，提出改进或合作的领域，并为与网络空间安全相关的政策决策提供了参考。

评估小组发现，在整个信息和通信基础设施发展过程中，各部门和机构的任务与职权是依据当时管理多样化和分散的技术及产业的法律和政策确定的。而由此产生的各项计划主要用于处理当时的特定问题，未必适应今天对数字化信息高度依赖的现实。

技术对国家和经济安全的影响促使联邦政府调整法律和组织机构，以适应形势发展。例如：

- 在 1918 年的一个联合决议案中，国会授权总统掌控美国所有电报系统，并根据需要在第一次世界大战期间使用电报系统。
- 1934 年《通信法》决定由联邦无线电通信委员会组建联邦通信委员会，并为所有电报和无线电通信建立完备的规章制度，对此类技术的后继发展产生了深远的影响。
- 1965 年《布鲁克斯法案》规定国家标准局——现在的商务部国家标准与技术研究所——负责制定自动数据处理标准和联邦计算机系统相关准则。
- 1984 年，第 12472 号行政命令重新将美国国家通信系统特许经营权赋予联邦政府，作为满足国家安全和应急备用之需的联邦电信财产。2003 年，美国国土安全部接管了美国国家通信系统的经营权。
- 1994 年，美国国务院根据《对外关系授权法》，负责管理与国际通信和信息政策有关的外交政策。

要解决“谁负责”的问题，就必须解决政府部门和机构间任务和职权分配问题，特别是在电信网络和互联网相互融合，以及其他基础设施部门日益依赖互联网，以实现互联互通的背景下，情况更是如此。将已经发展了一个多世纪的任务职责统一起来，这就要求联邦政府详细阐明政策，分清政府各部门和机构在网络安全方面各自的任务和责任。评估小组对 20 多个联邦政府部门和机构的反馈意见进行了分析，查明了网络安全相关政策存在的漏洞、重叠的任务职能和相互协作的机会。

随着威胁日益复杂，应对网络空间风险以及部门和机构间的沟通协作也因时而变。1998 年 5 月签署的第 63 号总统令规定，在白宫的直接领导下设立一个机构，指定牵头部门和机构，协调相关行动，并与民营企业相应部门合作，以“消除我们的重要基础设施——特别是

我们的网络系统——在防范和抵御物理和网络攻击方面存在的任何漏洞”。这项政策在 2003 年的《确保网络空间安全国家战略》文件中又进行了修订。

2003 年年底的第 7 号国家安全总统令进一步增强了这项工作。该命令赋予国土安全部全面协调国家重要基础设施——包括网络基础设施——的保护工作；可跨越所有部门与行政部门指定的具体机构进行合作。这两项政策的重点是防御性措施，第 7 号国家安全总统令并未包括保护联邦政府的信息系统。2007 年，《国家网络安全综合计划》采取了不同的策略，其核心是把过去分散的网络防御任务与执法、情报、反间谍和军事能力“衔接”起来，解决各种各样来自远程网络入侵和内部违规操作所造成的网络威胁，以弥补存在的一系列不足。《国家网络安全综合计划》的策略在第 54 号和第 23 号国家安全总统令中被定为法律，主要针对行政部门的网络安全。但行政部门的网络在美国所依赖的全球信息与通信基础设施中仅仅占很小的份额。

本报告总结了评估小组的调查结果，并介绍了有助于美国未来实现更可靠、有韧性、值得信赖的数字基础设施的一些初步步骤。它并未对各种选择或诸多计划的审核提供深入的分析。相反，它提出了需要加强协调和综合发展的政策。报告用 5 个主题详细地介绍了调查结果和行动方案：一是顶层领导，二是建设数字化国家的能力，三是共同负责网络安全，四是加强信息共享和应急反应，五是构筑未来架构。

四、从最高层实施领导

确保网络空间拥有足够韧性并值得信赖，以支持美国的经济增长、公民自由与隐私保护、国家安全和民主体制的完善，需要把网络安全列为国家头等大事。只有在政府最高层领导下才能完成这一重要而复杂的任务。

（一）由白宫实施领导

由白宫掌握网络安全相关政策的领导权并提升领导的层级，会向美国和国际社会发出明确的信号，即我们对网络安全问题的态度是非常严肃认真的。许多政府部门和机构，以及总统办事机构将需要协调不同的职责和权限，以有效地促进网络安全。目前，没有一个人或一个组织专门担负着协调联邦政府网络安全相关活动的职责。如果没有一个中央协调机制，没有及时更新的国家战略，没有各行政部门制定和协调的行动计划，以及没有国会的支持，靠单打独斗的工作方式不足以应付这一挑战。

政府行政部门早已经设立了一个由国家安全委员会和国土安全委员会共同领导的信息和通信基础设施跨部门政策委员会，作为解决有关网络问题的主要政策协调机构，以便获得可信、可靠、安全和长久的全球信息和通信基础设施及相关能力。

美国总统应该考虑再任命一名白宫网络安全政策官，该官员应向国家安全委员会和国家经济委员会报告，以协调全国范围内与网络安全有关的政策和活动。此官员将主管信息和通信基础设施跨部门政策委员会工作，加强与总统办事机构其他部门协调领导工作，解决各种优先任务和协调政府部门间网络安全政策和战略的发展。网络安全政策官应该参与所有相关的经济、反恐、科学与技术政策的讨论和研究，并制定网络安全长远规划。

要取得成功，总统网络安全政策官必须得到总统的全力支持，拥有权威和足够的资源，以便在政策制定和协调部门间的网络安全相关活动中有效地开展工作。其手下至少有国家安

全委员会的两名资深主任和适当的工作人员辅佐，并至少有一名国家经济委员会的资深主任和适量的工作人员为其工作。这些资深主任应通过网络安全政策官向上汇报工作，并共同致力于达成本报告所设定的目标及其他国家政策。此外，为促进国家安全委员会内部的整合，委员会中的每个地区主管局和职能局应当专设一名工作人员，负责本单位职能范围内的网络安全事务，并与国安会新设的网络安全局协调工作。

网络安全政策官不应拥有管理网络运营的责任或权力，也没有权力自己制定政策。网络安全政策官应当利用政府部门和机构间的协调程序，一切工作都要与联邦政府的首席技术官和首席信息官，以及管理与预算局、科学与技术政策办公室和国家经济委员会等相关部门进行商议，协调整个联邦政府有关网络安全的政策和技术工作，确保在总统的预算中能反映出网络安全工作是联邦政府的优先工作，并进入立法议程。

该网络安全政策官亦可被任命担任白宫网络应急反应行动官（其职能与白宫监控恐怖袭击和自然灾害的行动官员相类似），这一任命也将使美国更有效地进行危机管理；政府部门和机构将继续担负各自的网络运营职责。

为了便于协调，所有联邦政府部门和机构应该在各自内部设立一名联络官，负责协助白宫处理网络安全事务。

通过政府跨部门政策制定程序，网络安全政策官为总统起草新的国家战略，以确保信息和通信基础设施安全。这项战略应包括对《国家网络安全综合计划》落实情况的后续评估，并适当吸取其成功的经验。新国家战略应侧重于使高层领导集中精力和时间，消除阻挡美国实现拥有可信、可靠、安全和富有韧性的全球信息与通信基础设施以及相关能力的障碍。该战略将帮助政府努力提高公众意识，恢复和建立国际联盟及公私部门之间的伙伴关系，建立一个更加周全的国家网络应急反应与恢复计划，并采取积极的研究与发展计划，催生提高网络安全的新技术。

联邦政府应继续落实《国家网络安全综合计划》提出的“任务衔接”原则。政府各部门和机构应加强网络防御单位与负责美国网络空间作战的情报、军事和执法单位的合作，就网络威胁、网络交易、网络技术和网络存在弱点等问题进行交流，扩大网络经验、知识和观点的共享。此外，网络安全政策官应当帮助协调涉及网络空间的情报、军事政策和战略——包括打击网络恐怖主义，确保所有的任务有机融合在一起。网络安全政策官还应当与外部的咨询机构保持联系。许多咨询机构都涉足与网络安全相关的问题，这些机构包括国家安全和电信咨询委员会、国家基础设施咨询委员会、重要基础设施合作咨询委员会以及信息安全与隐私咨询委员会。网络安全政策官应审查这些机构的职能，并提出必要的改革建议使其咨询服务最优化，并杜绝不必要的重复。

为确保公民自由和隐私权利得到保护，还需要得到其他组织的帮助。这些组织将可以在政府网络安全计划和公民自由与隐私团体以及公众之间建立起信任，显示网络安全计划的透明，这在网络计划开始实施之初尤为重要。当务之急是要建立隐私与公民自由监督委员会，加快委员会成员的选举工作，并考虑是否寻求修订法案以扩大其工作范围——包括处理与网络安全有关的事务。其他可行的办法还包括：加强政府负责公民自由事务的部门与隐私顾问们就网络安全的政策问题进行定期沟通，或在国家安全委员会内任命一名负责隐私与公民自由事务的官员（或范围再大一些，在总统办事机构内任命一名负责隐私和公民自由权利的官员），与民营部门隐私与公民自由团体、隐私与公民自由监督委员会和政府负责隐私与公民

自由事务的官员进行协商。

与制定网络安全政策同样重要的是确保有效地执行和落实这项政策，以实现更远大的战略目标。因此，网络安全政策官同管理与预算局、总统办事机构其他部门协商，必须确保有效地落实网络安全相关政策和采取相关行动。在 60 天的评估期间，有关各方就协调和监督网络安全活动提出了各种各样的办法。一些评论家确信，强有力的行政领导，以及多年来政府部门和机构的努力，是确保美国政府拥有可以有效执行网络安全计划机制的重要基础。目前，一些网络安全监督职能都不是在总统办事机构领导下实现的。例如，由国家情报总监领导的跨部门联合网络特遣队，目前负责协调和监督执行《国家网络安全综合计划》。网络安全政策官通过同管理与预算局和总统办事机构其他部门协商，应该就组织机制调整提出建议，以实现相应的监督、执行和其他一些职能，包括在管理与预算局或总统办事机构建立一个拥有跨部门联合网络特遣队功能的机构，创立一个类似艾森豪威尔总统行动协调委员会的实体，或建立一些可协助评估联邦政府部门与机构表现和监督联邦政府网络安全标准遵守情况的组织机构。在这样一个办公室成立之前，跨部门联合网络特遣队将继续执行其任务。

（二）评估相关法律和政策

总统的网络安全政策官应与政府部门和机构合作，提供协调一致的政策指导，并在必要时详细说明整个联邦政府确保网络安全相关活动的职权、作用和责任。适用于信息和通信网络的法律是由宪法、国内法、国外法和国际法共同组成的一个复杂法律体系，这一体系制约着政策选择。在美国，这种组合在一起的法律混合体之所以存在，是因为联邦政府在整个信息和通信基础设施发展过程中，颁布了诸多法律和政策，以控制多样化的产业和技术。

由于传统的电信网络和互联网日益融为一体，以及其他基础设施领域日益将互联网作为互联互通的主要手段，法律和政策应当继续找出一种综合性方法，将保护公民自由、隐私权利、公共安全、国家和经济安全的利益与灵活多样的网络应用和网络服务所带来的好处结合起来。在一些领域中缺乏司法裁定既带来了机遇也带来了危险，决策者对此应充分理解——法院可以介入并规范法律的应用，特别是涉及宪法权利的领域。制定政策必然受到法律框架的规范和制约，而且在政策上深思熟虑有助于找出现行法律中存在的差距和争议，让我们知道必须做出的法律改进。这一过程可能会根据美国的法律原则提议组建新的立法框架，对加之于信息、通信、网络和技术上的相互重叠的法律进行合理调整，或对已有的法律进行新的诠释，使之适应技术变革与实现政治目标。不过，采用其中任一方式都会有风险，可能使联邦政府保护信息和通信基础设施的一些活动更加困难。

政府应适当地与国会进行有效合作，以确保拥有完备的法律、政策和资源用于完成美国网络安全相关工作。国会已对国家有关网络安全的需求表示关注，并决定由两党共同担任领导，政府将会从国会的知识和经验中获益。与政府部门和机构共同工作的网络安全政策官应与产业界进行协商，以便了解法律和政策给网络运营方面带来的影响。

（三）加强网络安全工作的联邦政府领导和责任制

在数字化时代，仅仅依靠白宫将不足以领导美国实现广泛的目标，整个联邦政府都必须担负起领导职责。将网络安全列入总统议事日程的优先项目、根据既定的目标审查政府部门和机构的网络安全工作进展等，有助于落实责任和推动工作进度。网络安全政策官——与国

家安全委员会、管理与预算局、国家经济委员会和科学与技术政策办公室协商——将界定工作进度和成功的标准，提高网络安全工作在所有机构预算中的“能见度”。

要使网络安全工作透明并对整个网络安全投资进行有效管理，管理与预算局应利用其项目评估机制，确保政府部门和机构在追求网络安全目标时有效使用预算。正规的网络安全项目评估机制可以使政府部门和机构详细说明每个计划的意图与目标，并建立是否达成目标的统一标准。《国家网络安全综合计划》已经成功地运用了一种类似的做法。

根据 2002 年《联邦信息安全管理法》的要求，政府部门和机构的领导人必须承担起责任。政府与国会共同努力，更新并强化这项法规。政府部门和机构的领导执行计划要求各部门和机构及时汇报在确保网络系统安全方面的工作进展情况。美国联邦政府应制定备选方案，支持政府部门和机构落实遵守网络安全政策的领导责任制，坚决执行相应的网络安全程序。

提升各级地方政府网络安全事务的领导层级。州、地方和原住民保留地政府应考虑把网络安全当成一件大事来抓，指定一名领导人专门负责，以确保首席信息官、首席信息安全官与州国土安全顾问之间的有效协调。评估小组从美国州长协会的代表那里听到一些反映，说网络安全是他们在保护各州重要基础设施资产工作中最薄弱的环节。州国土安全顾问可以从若干国土安全部批准的项目中开支，用于网络安全工作。但从历史来看，所提供的资金在很大程度上并没有优先用来确保网络安全。州、地方和原住民保留地政府应考虑是否应把网络安全当成一个大问题，并确保首席信息官、首席信息安全官与州国土安全顾问协调一致，保持强大的防御态势。

五、打造数字化国家的竞争力

国家正处于一个十字路口。计算机几乎改变了日常生活的一切，不论是在家中还是在工作场所。网上银行、网上购物和网上报税等都已非常普遍。国家的基础设施正在经历一场革命，数字化和网络技术不断通过大型系统进行整合，如智能电网和下一代空中交通系统。近期颁布的《美国复苏与再投资法案》中的内容鼓励发展现代信息和通信设施，以便提高美国的竞争能力，并使用技术来解决国家所面临的最为紧迫的问题。美国面临着双重挑战：在维护一个促进创新、开放式互连、经济繁荣、自由贸易及自由环境的同时，也要保证公众安全、公民自由和隐私。

大众需要明确了解技术的安全使用。另外，美国需要一个技术先进的工作组来维持其在 21 世纪的经济竞争力。在学校，数学和科学必须成为首选学科。美国应发起一项 K－12（注：指从幼儿园到高中的教育）网络安全教育计划，以便进行数字安全、道德和保护教育；扩展大学课程；并且为培养一支数字化时代的称职的劳动力队伍创造条件。正如总统曾提到的，“美国所面临的挑战中，让我们的孩子为全球经济竞争做好准备最为紧迫。”为了帮助完成这些目标，国家应该提高全民的网络安全风险意识；建立一个教育系统以促进对网络安全的了解，并让美国继续在信息技术的科研、工程和市场领域保持和扩大领先地位；扩展并培训用于保护国家竞争优势的劳动力队伍；帮助组织和个人在风险管理上做出明智的选择。

（一）提高公众意识

形成对网上活动风险以及如何对其进行管理的广泛的公众意识，需要制定一个有效的战

略。联邦政府应该与教育者及产业界部门一起，引导国家网络安全的公共意识和教育。总统网络安全政策官应该负责这一公众意识战略的制定并指导其执行，并且应寻求国会、联邦政府、地方与原住民保留地政府、民营部门及公民自由与隐私组织的支持。战略应该涉及对公众进行关于威胁和怎样提高数字化安全及道德的教育。恶意行为体经常利用人们通过互联网接收信息或提交个人信息的行为。因此，该行动应专注于公众信息以便提高对网络使用的责任心，并加强对欺诈、身份盗窃、网络掠夺及网络道德等方面的防范意识。过去在公共安全活动中的一些成功做法，如为了防火而设置的警示牌、推广使用汽车安全带的提示条等，都可以当做一个模本加以利用，以便通知和帮助公众认识到网络安全的重要性。这些公共服务行动应该注重培养儿童的网络安全意识，以及那些准备选择职业的高年级学生的意识。知名人士、同技术一同成长起来的一代及新型媒体，都可以在有效传递信息方面发挥重要作用。

（二）加强网络安全教育

大约在 1957 年 10 月苏联发射人造地球卫星之后的一段时期，美国处在一个以数学和科技技能为主的全球竞争之中。根据《经济学人》中的一则报道，出色的信息技术职业者“到处短缺，但是形势会更加严峻，因为所需技能的本质正在发生改变。除了技术知识以外，明天的信息技术职业者将要求在项目管理、变革管理和业务分析等方面具有专业知识”。这项研究指出，美国继续拥有世界上最好的信息技术公司运营环境，在教育、基础设施、创新鼓励和法律保护等多个重要领域均具有规模和质量优势，可帮助打造竞争力。然而，2007—2008 年关于计算机学位和入学趋势的“托比调查”显示，美国的计算机科学和工程学位毕业生比 2004 年的高峰时期减少了约一半。国家无法容忍这种衰退继续下去。

联邦政府以及全体机构应该扩大对关键教育计划和研发的支持，以便保证国家在信息时代经济中持续的竞争力。现有的计划应该加以升级，或者扩大，而且其他的活动可以作为额外的计划模式参考。例如，2006 年国家科学基金开始征集关于其“恢复计算机大学教育的途径”的建议。这个项目试图打造“具有计算机能力和技能的美国劳动力，以便推动 21 世纪国家的健康、安全和繁荣”。

作为直接激励措施，不仅为那些在网络安全教育领域追求进取的学生，同时也向那些立志在联邦政府获得相关职位的学生提供奖学金。国家科学基金会和国土安全部为 34 个大学的服务计划提供奖学金。超过 1000 名学生在该计划的前 8 年得到了支持，其中超过 80％的学生在联邦政府获得了工作。国家科学基金会强调，考虑到迫切需要壮大相应的劳动力队伍，加强研究和教育之间的协同作用再怎么强调也不为过。

国家信息安全教育与研究学术中心，由国家安全局于 1988 年创立，从 2004 年开始由国土安全部共同资助，在 38 个州和哥伦比亚特区的 94 所大学推行更高水平的信息安全教育。这些中心已经同众多知名大学建立了合作关系，包括一些社区、拉美族裔和传统黑人学院。国防部也对这些大学中的信息安全奖学金计划提供了赞助。

全国大学网络保护竞赛、美国数学奥林匹克协会、能源部科学杯以及西门子基金数学、科学和技术竞赛都提供了以竞赛为导向的范例。其他范例包括国家科学基金会援引国防先期研究计划局的重大挑战而组织的一个学术小组，马可姆波里奇国家奖，以及旨在建立高级加密标准的竞赛。

（三）扩充联邦信息技术劳动力队伍

总统网络安全政策官应同信息和通信设施联合部门委员会协作，考虑如何更好地吸引网络安全专业人才，并采取措施慰留联邦政府内拥有此类技能的职员。各个部门和机构已在吸引产业界人才方面获得了一些成功，但获取、转移或更新安全审查需要大量的时间，这造成了机会的流失。联邦职员还应该有机会丰富个人工作履历和促进自身职业发展，而单独某一家政府部门常常无法提供这类机会。展开共同培训、进行部门间轮岗，甚至与民营部门之间进行可能的岗位轮换不但是一项有效的做法，而且会有利于人才素质综合培养和专业人才库的建立。

（四）将提高网络安全视为企业领导责任

联邦政府应该继续促进在各级政府和产业界中关于威胁、漏洞和有效措施的计划和信息分享。只有信息技术劳动力队伍了解网络安全的重要性是不够的，各级政府和产业界领导需要根据现实和潜在风险，做出业务和投资决定。联邦、地方和原住民保留地政府面临着类似的问题。州政府经常起到革新孵化器的作用，因而可能会提供一些在管理信息和通信设施方面所得到的经验。联邦政府应该继续同产业界一起确认并发布在安全设计和信息技术产品经营方面的有效措施。

六、共同承担网络安全责任

如果联邦政府孤立地开展工作，那么联邦政府在许多方面都不可能确保网络空间的安全。关于这一点，公共与民营部门有着共同的利益，以确保为商业和政府服务提供一个安全、可靠的基础设施平台。政府和产业界领导者在国内和国际事务上，都需要界定角色与责任、整合各种能力并发现各自的问题，以便制定出整体的解决方案。只有通过这样的合作关系，美国才能够提高网络安全水平，获得数字革命所带来的全部效益。保证网络空间的安全，这一全球性的挑战要求各方做出更大的努力。这一努力应寻求同民营部门进行持续的协作，通过制定全球标准来提高可被共同使用的网络的安全，扩展法律系统打击网络犯罪的能力，继续发展并推广成功的实践经验，并保持稳定、有效的互联网治理。

（一）加强民营部门和政府间的合作关系

联邦政府有责任保护、捍卫国家，并且各级政府有责任确保其公民的安全与健康。然而，民营部门设计、建立、拥有以及运作的大多数网络基础设施同时为政府和私人用户提供支持。对于基础设施的安全性和可靠性以及通过这些设施所发生的交易，业界和政府承担着共同的责任，二者应该紧密合作以解决这些相互依赖性问题。联邦政府可以采取多种不同的手段来应对这些挑战，其中有些可能要求修改相应的法律和政策。

民营部门应帮助弥补执法和国家安全的局限性问题。当前的法律允许使用某些工具来保护政府网络，但不是民营网络。产业界领导者可以利用企业信息共享来帮助说明数据泄露、工业间谍活动及服务能力丧失或降低给公司带来的风险以及对盈利能力的影响。产业界领导者可以要求销售商和服务供应商提供更多保证，同时承担起开发更加安全的软件和设备的责任。企业应想出有效的途径，以便在彼此以及联邦政府之间分享检测方法、关于违规和攻击

方法的信息、修复技术及取证能力。

如果风险和后果可以以货币价值的形式来衡量，那么各个机构就将拥有更大的能力和动力去解决网络安全问题。尤其是民营部门经常试图通过业务个案来证明以下两方面所需的资源支出的合理性：一是把信息与通信系统安全整合到公司的风险管理之中，二是建立可以缓解风险的伙伴关系。政府可以考虑利用以激励为主的立法或监管工具来协助形成好的价值取向，并且帮助培养一个可以促进并鼓励伙伴关系和信息共享的环境。

总统网络安全政策官应同相关部门机构及民营部门进行合作，共同考察现有的政府与民间伙伴关系和信息共享机制，以便识别或建立最为有效的模型。过去十多年以来，公私伙伴关系促进了信息共享，并为美国重要基础设施保护和网络安全政策奠定了基础。在这一时期，联邦政府和民营部门共同建立了大量有关网络安全和信息与通信设施问题的论坛。

这些团体作了很多贡献，但是由于精力分散，已使一些参与者对缺乏明确界定的角色和责任、各团体之间参差不齐的能力以及不断增加的计划和建议，感到灰心丧气。结果，政府和民营部门的人员、时间及资源被大量浪费于重复、不连贯的工作中。伙伴关系必须进行转变，以便明确界定这一关系的性质、不同团体及其参与者的角色和责任、对各方贡献的期望，以及责任机制。联邦政府应对各种资源进行优化、调整，然后把它们提供给现有的组织，以此来完善其识别优先等级的能力，实现更加有效的执行效率并制定响应与恢复计划。

为期 60 天的评估考察了大量有效的政府与民间伙伴关系模型。尽管这些模型功能差异很大，但它们却共享着某些重要的特性。每一个模型都有一个定义明确的机构使命、参与者的角色和责任，以及清晰的鼓励参与的价值取向。通过在成员之间培养并维持一种相互信任的氛围，每一模型都可以减轻担忧，否则这些担忧可能会妨碍参与。现有的网络安全伙伴关系也许会应用这些模型所具有的那些最为有效的特征。

（二）评估妨碍政府与民间伙伴关系转变的潜在障碍

民营部门中的有些成员一直担心，某些联邦法律也许会妨碍民营部门和政府之间全面协作性质的伙伴关系及运作信息共享。例如，业界中的有些人担心在现有的伙伴关系模型中，同一领域成员之间进行的信息共享和统一规划，也许会被认为同禁止贸易限制的法律“互相串通”相抵触。业界还表示会有所保留地向联邦政府透露敏感性或专有的商业信息，如弱点和数据或网络漏洞。这种担忧一直存在着，即便相关的法令对此给予了保护，如《商业机密法》和《关键基础设施信息法》。这两项法律的颁布旨在消除产业界对于《信息自由法》的担忧。除了这些问题以外，产业界也许还会担心共享信息所带来的名誉损害、责任或管制影响。相反，鉴于对敏感的情报来源和方法或者个人的隐私权利的法律保护，联邦政府有时会限制政府与民营部门共享的信息。

这些担忧并不是孤立存在的。面对不公平竞争，各种反垄断法律提供了重要的安全保障，并且《信息自由法》将协助确保政府的透明性，这对于维持公众信心至关重要。公民自由和隐私团体表示，担心不断扩展的保护措施只不过是一块逃避责任的合法盾牌。此外，信息与通信市场的全球性特点会使信息共享的挑战变得更加复杂。如果在美国运营的产业界成员是外国公司，那么强制性的信息共享或排斥此类公司加入信息共享体制，可能会对贸易产生影响。

政府应同民营部门进行创造性的合作，以便找出恰当的解决方案——同时照顾到交流信

息和保护公共与私人利益这两个方面的要求，从而采用统筹兼顾的方法解决国家安全和经济安全问题。这些解决方案应该识别出明确的、可执行的信息共享目标，并制定事件报告标准。民营部门将更乐于分享那些不需要更改数据所有权的解决方案，如英国模型中的做法：选择经过审核的信息安全提供方而不是政府作为合并数据的链接点。

最后，联邦政府应该请学术界、公民自由与隐私团体、开放政府的提倡者以及消费者积极参与，以确保政府政策充分考虑到了这些群体所代表的广泛利益。几乎没有什么问题可以简单地看做一个孤立的程序、政策或技术问题。技术的变化通常会成为政策制定的考虑要素，也许会要求改变现有的程序。政策改变（如规章或税收鼓励措施的通过）可以影响到采购或技术研发方面的决定。联邦政府还可以考虑这样的方式：它能够把更多的资源集中到可能“改变产业界格局”的领域的研究上，例如，行为与政策方面以及以激励为主的网络安全解决方案。鉴于这些问题的密切相关性，更需要确保所有利益攸关方的利益都得到体现。

（三）与国际社会进行有效的合作

国际规范对于建造安全、稳定的数字基础设施来说至关重要。美国需要制定一项战略，以便打造国际环境并把对一系列问题有着类似观点的国家聚集在一起，这些问题包括有关领土管辖权、主权责任及武力使用等可以接受的规范。此外，不同国家与地区的法律和实践（例如，涉及以下多个方面的各种法律：网络犯罪的调查和起诉、数据保存、保护与隐私，以及网络防御和网络攻击响应的途径），为打造一个安全、安定并具有韧性的环境带来了巨大的挑战。要解决这些问题需要美国同所有国家以及国际机构、军事同盟与情报伙伴进行合作，包括发展中国家，它们在构建其数字经济与设施的过程中也面临着这些问题。

在过去十年中，联邦的通信、基础设施和网络安全相关的政策都是沿着不同的道路发展的。采用更加综合的政策制定方法可以确保制定相互支持的目标，并可以让美国通过更为有效、恰当的立场把握其国际机遇。对于一系列独立领域（包括网络安全和对言论自由及其他公民自由的保护）的国家利益，美国应采用综合的解决方法，以便制定一贯的政策。

总统网络安全政策官应与各部门和机构合作，加强并整合机构间制定及调整国际网络安全立场的流程。此外，联邦政府在继续同民营部门长期合作的同时，应制定一套积极参与计划以供国际标准机构使用。这其中应包括对现有政策的评估，并对立场的确定、完善或重申进行协调，从而确保与网络安全相关的经济、国家安全、公共安全和隐私利益都被考虑在内。包括联合国、八国集团、北大西洋公约组织、欧洲理事会、亚太经合组织、美洲国家组织、经济合作与发展组织、国际电信联盟、国际标准化组织在内的十多家机构都致力于解决信息和通信基础设施方面的问题。新组织正开始考虑与网络安全相关的政策和活动，其他组织也在拓展现有的工作范围。这些机构所考察的政策和所开展的活动有时会彼此冲突，并经常重合。这些组织公布的协议、标准或实践都具有不可忽视的全球影响力。它们的绝对数量、类型，以及这些地区不同的侧重点超出了包括美国在内的许多政府的应对能力。

总统网络安全政策官应与各部门机构合作，加强其对国际立场、磋商和讨论的识别、跟踪和优化的能力，与网络安全相关的协议、标准、活动和政策都是在这些过程中形成的。以往的经验表明，美国需要继续参与一系列的国际活动。联邦政府应与民营部门及其他国家密切合作，以确保各成员充分参与到相应的论坛之中，就关乎美国未来全球信息和通信基础设施利益最重要的问题进行讨论。美国及其国际盟友应利用参与区域或其他论坛的机遇，促成

共同的政策目标，关注现有国际组织的工作，并减少重复性的工作。例如，国际电信联盟和国际标准化组织都在从事网络安全取证标准的制定。对于主题更为宽泛的论坛，美国也应寻求机会，以促进相关项目中有关信息和通信基础设施的安全和发展。联邦政府应与民营部门共同协调和发展国际伙伴关系，以应对信息和通信基础设施相关的一系列网络安全方面的活动、政策和机遇，这些基础设施是美国商业、政府服务、美国军队以及国家的根本所在。政府和产业界间新签署的协议应加以备案，以促进国际信息共享和战略运营合作。对于指导对外发展及发展海外能力，联邦政府应增加资源并提高警惕。例如，美国应加快步伐帮助其他国家建立法律框架、提高打击网络犯罪的能力，并且继续推广网络安全方面的准则和标准。美国也应与其盟友合作，确保互联网的稳定性和国际互用性，同时提高互联网的安全性和可靠性，使所有用户受益。

七、建立有效的信息共享和事故响应框架

美国需要建立一个全面的框架，以便协调政府、民营部门和盟国共同应对重大的网络事故。联邦、州、地方及原住民保留地政府应与业界合作，提前完善其正用于检测、预防及应对重大网络安全事件的计划和资源。由于此类事件可能影响到政府和产业界部门之间的互联网络，因而在重大事件发生之前、期间和之后，对此类计划和行动进行协调就显得特别重要。例如，尽管收到关于 Conficker 蠕虫病毒的提前预警和网络防御的指示，但如果蠕虫病毒在 2009 年 4 月 1 日激活时附带恶意的有效负载，那么一些联邦部门和机构就无法应对。

（一）建立事故响应框架

与其他重大国家事故一样，在发生重大网络事故时，只有白宫有权协调与事故响应相关的一系列职能部门和权力机构。各部门和机构应按白宫总体战略方向履行各自责任。总统网络安全政策官应为白宫网络事故应急的执行官（其职能与帮助白宫检测恐怖主义袭击或自然灾害的执行官类似）。

联邦政府应建立一套明确且具权威性的网络事故响应框架，该框架在修改后的《国家响应框架之网络事故附件》中备案。到目前为止，针对网络事故的联邦响应还未统一。对于涉及国家安全/应急准备通信的情况，第 12472 号美国总统令明确了现存的职能部门和处理流程；然而，根据当前的法律政策，各部门和机构仍各自负责决定和实施隔离、保护和恢复自身计算机网络和数据的措施。

由于国家安全和其他联邦网络之间现存的法律而非人为差异，联邦网络事故响应的责任分散到了不同的联邦部门和机构之中。根据事件的性质，例如，重大的漏洞、犯罪袭击或军事事件，不同部门或机构可能负有或承担着主要的应急责任，而其他部门或机构则可能对此一无所知。另外，对整个事故的责任分配可能还不明确。尽管每个参与者都有着明确的专长领域和合法权利，但它们很难统一到一个单一的协调框架中。把任何权力部门合并到一个统一架构中可能都需要通过法律来实现。信息和通信设施联合部门委员会进程应明确同事故响应相关的不同部门和机构的角色、职责及资源，必要时对其协调或补充；了解事故响应的各个方面如网络安全、执法、情报及军事等部门及其各自的优势。

众多评论家强调建立事故报告和响应门槛的重要性。网络运营商和服务提供商每天都会处理大量尚未达到“滋扰”级别的事件。在这些低级别事故中，藏匿有相对少量的可能产生

巨大影响的入侵或攻击。其他政府和民营部门的网络运营商很想了解此类事件的技术细节，以帮助其抵御相似的网络威胁；执法部门和情报机构也可借此跟踪并寻求方法制止网络安全方面的犯罪和来自国外的威胁活动。

互联网由管理运作和为客户提供服务的企业联合运营。网络运营商建立和维护信息通信基础设施，为客户提供接入和宽带服务。服务提供商提供互联网接入网关、安全服务、存储或处理服务，以及信息的获取（如互联网地址或新闻）和应用设备（如搜索引擎）。单个公司可提供独特的接入、信息和服务的混合组合（如社交网络）。

联邦政府应与州、地方和原住民保留地政府及业界合作，总结一系列威胁情况和衡量指标，以供风险管理决策、制定恢复计划及确定研发优先顺序。同时应发展建模和模拟能力，以帮助演练这些计划并确定可能的破坏级别。

信息和通信设施联合部门委员会应在各部门和机构中建立明晰、可执行的事件即时汇报规则，以便提高机构间响应的效率。各部门和机构在各自管辖范围外的事件汇报存在差异，其对重大事件的即时汇报将使联邦的整体应急响应受益。

总统网络安全政策官应与信息和通信设施联合部门委员会合作，确定发展和保持态势感知和事故响应能力的最有效方法。《国家网络安全综合计划》应继续致力于提高联邦网络的防御能力，同时考虑调整实施计划或增添内容的需要。总统网络安全政策官尤其应该做好以下几方面工作。

- 与民营部门合作，探索如何更好地将技术能力应用到国家基础设施的防御中，以及需要什么样的法律框架来保障隐私权和公民自由。
- 审议国家网络安全中心的运作理念及其实施，决定该中心关于责任、资源战略和管理的提议是否充分，使其能够提供支持网络事故响应努力所必需的态势感知共享信息。
- 继续向可信任的互联网接入项目的目标迈进，减少政府网络接入的数量，同时根据对挑战的现实评估，再次考虑项目中的目标和时间表。在过去的两年里，一些部门和机构在减少接入数量和部署系统上取得了进步，这些系统将帮助联邦政府阻止并检测恶意的行为。然而，政府在充分发挥能力之前仍然有很多工作要做，而且可能需要考虑额外的政策以促进战略的全面实施。
- 为了联邦网络的利益，适当评估并与公民自由和隐私团体继续协商进行入侵检测和防御系统的试点部署工作，评估这些系统的性能，并且继续研究若将这些系统应用到州政府系统中会产生的问题。（系统中的）传感器将对联邦网络获得态势感知信息具有关键作用；随着这些部署工作的进行，政府也将从政策、法律或技术层面受益。
- 探索——与业界、公民自由和隐私团体协作——其他长期的入侵检测和防御体系建构。

联邦政府应提高自身向总统提供网络入侵或攻击的战略预警的能力。联邦政府应继续利用国家为促进密码技术、信息保障技术和必要配套设施的根本发展的投资。这些投资以及其他的情报能力，对于网络攻击的战略预警至关重要。此外，联邦政府应找出执法能力上的差距，或保护国家基础设施所建立的调查权威。所有新设的权威部门须始终保障公民自由和隐私权。

美国政府应投资有助于防御网络应急事件的流程、技术和基础设施。内容包括增加安全检测，投资网络管理自动化或中央化系统，以及对某些非保密系统实施更严格的互联网接入。

政府需要建立一套可靠持续的机制，以便将所有适宜信息整合在一起，形成一张共同的运行图。联邦网络安全中心经常分享彼此的信息，但其中没有一家机构可以将来自不同中心和其他资源处得到的所有信息综合起来，制成一张不断更新且涵盖网络威胁和网络状况的全局图，以预报迫在眉睫的应急事故，以及支持协调事故响应。国防部负责整合关于网络健康和状况、入侵企图和对自身网络的攻击的信息；情报界负责自身网络；国土安全部美国电脑应急反应小组负责民事联邦机构，以及在某种程度上对民营部门负责；执法和情报机构收集与网络有关的犯罪和国外威胁活动证据，但也需要具有处理有一定规模的犯罪活动的额外能力。

联邦政府应考虑若信息和通信基础设施遭受重大损害，尤其是当信息和通信网络融为一体时，是否有充足的可用替代品或通信设施储备。基础设施的替换或修复也要求有额外的计划和资源，尤其是当网络或电网中难以替换的元件受到物理损害时。

联邦政府应利用现有资源，在各级政府和民营部门间建立有助于防御、检测和应对网络应急事件的流程。联邦政府应利用州际信息共享和分析中心、全国 58 座州立和地方融合中心等现有资源，帮助树立信息和通信基础设施方面的态势感知意识。

（二）加强信息共享，提高事故应对能力

信息是防御、检测和应对网络事故的关键。网络软硬件提供商、网络运营商、数据拥有者、安全服务提供商以及某些情况下的执法或情报机构可能各自拥有信息。这些信息能够帮助检测和了解复杂的入侵或攻击问题。只有将上述各类信息来源整合起来，才有可能全面了解事故并做出有效的响应，使所有人受益。

联邦政府应与州、地方和原住民保留地政府及民营部门（包括数据拥有者、网络运营商及隐私和公民自由专家）合作，寻求网络安全方面的信息共享方案，消除有关隐私和专有信息的担忧，使信息共享符合国家的利益，达到互利的目的。鉴于民营企业关心其信息的潜在使用问题，政府必须保障其隐私权，做到执法公正，保护情报来源和方法，以及可能导致不公平竞争优势的政府信息。为了解决这些担忧，政府和民营部门都需要做到透明、诚信。可选方案包括以下几方面。

设立一个政府和民营部门都信任的第三方非营利性非政府组织，作为政府和民营部门共享信息的平台，以此提高政府和民营部门之间的关键网络安全性。此类组织可使用商业服务，并且不会扰乱日益壮大的安全服务市场。

联邦政府（如执法机构）与个体公司或公司集团（可能还有州、地方和原住民保留地政府的参与）之间持续的约束，在特定的部门或区域内实现一定程度自愿性的信息共享，超越在更广泛的背景下实现的信息共享。

美国政府应与受影响方和国会协商，考虑制定适当的信息共享激励措施。作为最后的手段，这些措施可包括综合方案中的监管措施，以满足社会对健全和具有韧性的关键基础设施的利益需求，保障公民自由和隐私权，维护作为美国经济系统基础的、公正公开的经济市场。加密或控制接入认证等强化隐私保障技术可减少信息共享中的某些风险。

联邦政府应全面评估妨碍网络安全信息共享的有关安全分级和人员涉密等方面的政策，

同时寻求信息共享改善方案，并确保公民自由和隐私权得到保障，敏感信息得到适宜的保护。联邦政府各部门和机构当前关于信息收集、使用、保留和散布的政策在很大程度上都是基于法定权限、对隐私和公民自由的关注、对来源和方法的担心以及历史惯例而来的。这些政策严重阻碍了联邦政府间的网络安全信息共享。此次评估应将联邦政府通过安全性和适用性改革倡议所取得的进展考虑在内，同时也要考虑信息共享环境在检查安全和适用性处理组件的所有方面时所做出的努力。

联邦政府应与民营部门合作，制定民营部门网络运营商向联邦政府进行事件汇报的标准。业界表达了作为受害者对汇报其网络事故的担心，包括随之而来的股东的担忧、市场反应或监管行动所带来的潜在消极影响。一家业内机构提议成立政府—企业工作组，设立具体到部门的网络事件门槛，以保证将信息汇报给安全官员。须制定相应的规则并监督政府对此类信息的使用，以保障隐私权和公民自由。另一完善报告程序的途径是考虑适当的数据破坏通知法案，要求企业将相关信息通知给公众和政府，其中包括可进行调查的执法部门。联邦政府也应检查已有的市场监管汇报规定的有效性和工作范围。与此同时，联邦政府须制定与民营部门进行事件汇报共享的流程和规则。这些规则的制定须考虑事件的分类和隐私问题。另外，联邦政府应协助研究团体获得网络安全事件的数据，并对此加以适当控制。这些数据可用来开发工具、测试理论和制定可行性解决方案。此类共享需要解决关于敏感或专有数据及个人身份信息的保护问题。

联邦政府应努力扩大与主要盟友在网络事件和漏洞方面的信息共享，寻求改善网络安全的双边或多边安排，并确保这些安排符合美国其他方面的经济和安全利益，使公民自由和隐私权得到保障。国际合作为美国政府与民营部门的合作带来了更多挑战。若美国政府计划与其他国家共享美国民营企业的行业信息，则国内合法的民营部门关于信息共享的担忧将会增加。民营部门和联邦政府再次需要做到明晰和诚信，以控制、散发和使用民营部门与政府共享的信息，包括对使用美国和国际社会之间共享信息的理解。

（三）提高所有基础设施的网络安全性

联邦政府应与民营部门合作，明确政府与民间伙伴关系的职能，以做好私有关键基础设施和重要资源的防御工作。联邦政府的核心责任之一即是共同保护私有关键基础设施不受武装攻击、物理入侵或国外军事力量、国际恐怖分子的破坏。同样，政府也在保护这些基础设施不受罪犯或国内恐怖分子的破坏上发挥着重要作用。然而，若攻击是通过计算机网络远程进行而非直接的物理行为，那么政府应对相同行为人，对相同基础设施施加的相同损害负多大程度的责任，这个问题尚未解决。大多数网络运营商和服务提供商都将自身网络的维护和防御工作归为自己的责任，但民营部门的重要组织已表示，业界希望形成一个工作框架，在此框架下政府将追捕恶意行为人，为民营部门运营商提供信息和技术支持，帮助民营部门保护自身网络。

在网络安全解决方案的制定过程中，联邦政府应考虑出台鼓励集体行动和竞争的激励措施。例如，网络空间至今还未出现“照顾标准”的法律概念。可能的激励措施包括调整法律责任（安全改善后责任减少，安全条件差则导致责任增加）、补充赔偿、税收鼓励政策，以及新的监管规定和执行机制。

总统网络安全政策官应与各级政府、民营部门及国际伙伴合作，制定战略和计划，鼓励

创新型网络安全解决方案，确保基础设施系统的安全和韧性。基础设施范例包括以下几方面。

政府应协助世界银行、国际货币基金组织等国际金融机构，向其提供必要的信息、工具及专业知识，并鼓励其运用最佳准则来保护自身的信息系统。2008 年这些机构的系统曾遭受一系列的严重入侵。

《美国复苏与再投资法案》通过储备基金来推广医疗信息技术的使用。随着电子记录保存（系统）在互联网上的日益普及和获取这些信息的便利性，病人信息的保护工作将事关美国政府可否得到公众的认可。

能源部应与联邦能源监管委员会合作决定是否需要为能源方面的工业控制系统另行制定安全执行令和程序。另外，随着新的智能网技术在美国的普及，联邦政府需要制定和通过相应的安全标准，以避免为对手制造可乘之机，侵入上述系统或对其发动大规模攻击。

交通部下属的美国联邦航空管理局在维持现有系统的同时，已制定了向下一代空中交通控制系统过渡的长期计划。交通部检察长于 2009 年 3 月 18 日在众议院航空交通和基础设施小组委员会上作证时称，需要评估潜在的安全漏洞，制定一套健全的网络安全战略和设计方案。

八、鼓励创新

基础设施必须具有一定的恢复能力以防物理破坏、非法操作和电子攻击。除了对本身信息的保护，减轻网络空间风险的战略必须侧重于访问基础设施的设备、基础设施提供的服务、网络的支持要素，以及所有用于移动、存储和处理信息的手段。这一战略还必须包括预防、减缓和应对针对运营并受益于基础设施的人员所遭受的威胁或破坏，运营或利用基础设施的程序，以及用于建造并维护基础设施的供应链。

信息与通信部门正在创建一个聚合平台，在此平台上数据、音频和视频应用占用共同的基础设施。当前国际互联网模型的分散性质，允许个人和企业家在无须得到许可的情况下，开发并配置创新的应用程序。创新带动了价值数十亿美元的新型业务，它们彻底改变了用户与网络及用户彼此之间的互动方式。随着科技对美国越来越重要，对于这一不断演变发展的基础设施，保持信心和信任至关重要。总统已呼吁联邦政府同业界保持合作，共同开发“下一代的安全计算机和应用于国家安全的网络互连”，制定“新的、严格的网络安全与物理恢复力新标准”，以及“保护个人数据的标准”。

美国应充分利用技术创新以便消除网络安全担忧。虽然市场上早就存在着许多可以明显增强安全性的技术和网络管理的解决方案，但由于成本或复杂的原因，这些技术和解决方案并没有得到广泛的使用。另外，鉴于国际互联网基础设施的内在设计，现有的解决方案已发挥到了极限，无法再继续提高。从长远来看，开放和创新将有助于建立透明且责任明晰的更加强大的基础设施。联邦政策必须满足国家安全要求，保护知识产权，并且要保持基础设施的可用性和连续性——即便在其遭受强劲对手攻击的情况下。联邦政府还必须注意不要制定一些不必要的政策与规章，它们可能会妨碍创新、导致低效率或使安全性降低。

（一）未来

2006 年的国家研究院报告《振兴美国的通信研究》指出：“通信网络是庞大、复杂的系统，其可靠性、安全性及演化性取决于连贯的、构思良好的架构概念的发展。”这一报告还

指出：“有多家厂商的产品被用来配置美国的电信基础设施并提供服务……（它们）超越了供应商的服务范围。由于业界正朝着水平结构发展，并且其分解出了大量的小型公司，不论是厂商还是服务提供商都不会准备去负责终端对终端系统的设计。”

这样一来，在处理政策、标准、研究、市场开发或采购问题时，就没有可以用来指导民营部门、学术界和政府做决定的统一建议。联邦政府、民营部门及其他利益攸关方应共同制定未来基础设施的技术中立的性能和安全目标，既满足其作为消费者的自身需求，同时又发挥其作为公众利益管理人的作用。联邦政府同其合作伙伴应针对具体的部门和组织，分别制定一系列综合的全国信息与通信基础设施目标。这些目标可以参考不同的计算平台模型或网络控制概念，以及通过政府、学术界或业界的研究项目产生的技术解决方案。

数据和服务向第三方联网服务器的移动被称为“云”，这为全球的民营部门和政府带来了新的政策挑战。跨越司法管辖边界的数据移动带来了以下三方面的挑战：法律执行、不同国家分别制定的隐私与公民自由保护，以及出现数据或网络漏洞时的决策责任。有些客户会试图限制服务提供商移动或存储数据的地点，而另一些跨国经营客户则会寻求利用地理和时区的差异性。

众多的机构和部门都在努力制定某些科技或基础设施部门的远景规划。例如，美国能源部与业界合作于 2005 年推出了一个为期 10 年的路线图，以便发展用于电网的控制系统。这一计划期望达到的目标是，截至 2015 年，“将实现关键应用控制系统的设计、安装、运作和维护，以便能够承受蓄意的网络攻击，同时不会丧失重要的功能”。国防部先期研究计划局的顾问小组把对当前基于《互联网协议》的网络防御称为一项亏本的买卖，呼吁“对可供选择的基础设施进行单独的考察”，从而完成对最佳候选基础设施的实验与评估。根据 2009 年 3 月的一份简报，国防部先期研究计划局正进行一项为期 6 个月的候选基础设施分析。

研发框架与基础设施开发的结合在总统网络安全政策官的领导下，联邦政府应与其他的总统办事机构部门及信息和通信设施联合部门委员会进行合作，提供研究与开发战略——专注于可以实现基础设施目标的、具有变革意义的技术框架，进一步完善当前的网络和信息技术研发战略及其他与研发相关的工作。联邦政府应扩大这些战略同业界与学术研究努力的协调，以便避免重复性的工作，利用具有互补性的功能和议事日程并使之同步，并且确保实现该技术换代并进入市场。

为了提高美国的竞争力，联邦政府应与业界合作，共同制定换代路径和刺激措施以便快速促进研究与技术开发，包括鼓励学术界与业界实验室之间的协作。

联邦政府还应与民营部门及其他利益攸关方合作，利用基础设施目标和研发框架为国家与国际标准机构制定目标。

（二）建立身份管理

如果不能提高认证水平，我们就无法提高网络安全性。身份管理不只是用于人员认证。认证机制还可以帮助确保在线交易仅涉及那些对于网络和设备而言可以信任的数据、硬件和软件的交易。尽管大多数系统今天都适于进行网络交易，但人们用于建立信任的电子提示技术等也许还没出现、不完整或者难于理解，起不到应有的作用。身份管理也许能够为可信任社团的个人和组织提供帮助，这些社团都是基于不同程度的身份公开和彼此约定的责任制而建立的。同时，它还可以排除不受欢迎的入侵者或不适当的会员请求。身份管理通过对个人

识别信息的发布进行额外的保护，还可能提高隐私水平。

联邦政府应与业界及公民自由与隐私社团合作，共同制定一个基于网络安全的国家身份管理构想与战略，为此需要考察一系列的方法，包括提高隐私水平的技术。联邦政府必须通过大量的信息、服务与福利计划同公民展开互动。这样一来，政府才会对保护公众的隐私信息产生兴趣。在线交易变得日益普遍，涉及金融、卫生与商业等诸多方面，需要一个在交易方之间建立信任的基础。

对于高附加值的业务（如智能电网），国家应该建立一系列可以选择加入的、能够相互配合的身份管理系统，以便为在线交易建立信任并提高隐私水平。

国家科学技术委员会下设的生物测定和身份管理附属委员会于 2008 年发布了一项报告，该报告提供了一个未来联邦身份管理构想以及一系列的研究与开发建议。联邦政府应把这项报告作为身份管理战略的一个出发点。

联邦政府应与国际伙伴进行合作，共同制定相关的政策，鼓励发展可以信任的全球体系，这种系统需要保护隐私权和公民自由并控制旨在保护公民与基础设施的法律实施活动的适当利用。

在国土安全第 12 号总统令的指导下，联邦政府正寻求在联邦事业中运用可相互通用的联邦身份认证机制。联邦政府应确保在联邦机构全面落实第 12 号总统令时，相关的资源都是可以利用的。联邦政府还应考虑让以下两方在国家紧急状态期间也能够使用联邦身份管理系统：重要基础设施的运营商，以及民营部门紧急响应与维修服务提供商。

（三）全球化政策与供应链的整合

信息技术革命及自由贸易政策带来的结果之一，是为在全球范围内分布有设备设施的公司建立了一个全球性的环境，用于其信息与通信产品的研究、设计、制造与服务。这一全球市场通过为美国的高科技商品和服务打开世界范围内的市场，给美国创造了巨大的利益。然而，新的制造、设计与研究中心在全球范围内的出现，使人们更加担忧微小的硬件或软件操作会更加轻易地导致计算机和网络的崩溃。仿造产品已带来了非常明显的供应问题，但记录在案的明确、蓄意的破坏的例子却很少存在。

需要对风险管理进行一种广泛的整体分析，而不是全面地否定外国产品与服务。供应链攻击所面临的挑战是，老练的对手也许会缩小目标范围，仅专注于特殊的系统，这样基本上就会使操作变得让人无从察觉。国外制造的确会给民族国家的对手带来更加容易的破坏产品的机会，但是，通过招募重要的内线人员或其他的间谍活动，也可以实现同样的目标。

最好的防御也许是通过持续创新来保证美国的市场领导地位。创新可以提高美国的市场领导地位，并且促进在维护具有弹性的、多样化的供应链与基础设施方面的最佳实践的应用。总统网络安全政策官与各部门机构应采取以下措施。

- 以国家安全局为国防部所做的工作为基础，通过综合服务管理局制定商业产品与服务的采购战略，以便建立市场激励机制，使安全成为硬件与软件产品设计、新的安全技术及安全的托管服务的一部分。
- 扩大同州、地方与原住民保留地政府及国际合作伙伴的合作关系，以便使这些采购的市场影响最大化。
- 同国会一起识别相关的机制，以便能够让各部门机构在适当的特定情形下，在做出

购买决定时考虑到相关的威胁信息。

- 从经济和威胁的角度出发，与业界一起提供威胁信息并确认管理供应链和内部风险的最佳方案。

（四）保持国家安全/应急准备的能力

联邦政府保护美国民众和提供共同防御的义务，包括负责确保国家在危机时刻能够进行通信并做出响应。通信系统可能会最先遭受此类事件的冲击，因此必须具有可以恢复的韧性或能力，以便做出响应并保护政府的职能。《1934 年通信法》授权在国家处于从“公共危险”到“战争”的不同警戒等级时，如果总统认为有必要维护国家安全或防御并且存在必要的临界条件，他可以运用、控制或者中止联邦通信委员会管辖下的通信服务、系统和网络。第 12472 号行政命令要求建立一个政府和业界联合的国家协调中心，以便为通信服务或设施在所有危机或紧急情况下的启动、协调、恢复或重建提供帮助。关于“国家连续性政策”（2007 年 5 月 4 日）的国家安全第 51 号总统令暨国土安全第 20 号总统令在联邦政府内对有关连续性通信的职责进行了分配。

国土安全部正在努力朝着这一目标前进：帮助国家安全和紧急状况用户提供下一代网络的聚合信息服务，并确保在各种灾难及其他会致使公众用户遭受通信服务严重恶化或中断的事件期间，其所提供的服务具有极大成功的可能性。下一代网络在国家安全方面的改进将包括数据、音频与视频等多种服务。主要运营商和服务提供商所构想的各种架构具有较大差异，这会使国土安全部的努力变得复杂化。为此，国土安全部正在考察、比较不同的方案，并争取在提交给标准组织进行考核的方案上与业界达成一致。联邦政府应针对下一代网络的国家安全与应急准备通信的能力，制定一个协调计划，包括进度时刻表与经费开支要求；提供联邦政府可以获取的附加服务的选择，或者引导政府将用在信息与通信基础设施上的投资用于提高在自然灾害、危机或冲突时期通信设施的存活性；与国际合作伙伴与标准制定机构进行配合，以便在遍布全球范围内的下一代网络环境中维护下一代国家安全/应急准备的通信能力；确保与行政部门连续性通信基础设施和下一代服务计划的开发相关的努力得到足够的人力资源支持。

九、行动计划

（一）近期行动建议

（1）任命一名网络安全政策官，负责协调全国的网络安全政策与活动；该官员同时具有国家安全委员会和国家经济委员会双重职责。在国家安全委员会内增设一个职能强大的部门，在网络安全政策官的领导下，协调政府部门间的网络安全战略和政策的制定。

（2）为总统批准实行确保信息和通信基础设施安全的最新国家战略做好准备。这一战略应包括对《国家网络安全综合计划》落实情况的评估，明确可以进一步发挥其成功经验的相关领域。

（3）将网络安全列为总统议事日程的优先项目，并制定工作业绩指标。

（4）在增设的国家安全委员会网络安全局中指派一名官员，负责公民隐私和自由权利事务。

（5）召集政府相关机构，就在制定政策过程中遇到的网络安全相关事宜进行清除跨越部门界限的法律分析研究；并制定统一的政策指导，以明确政府各部门网络安全工作的任务、职责和权限。

（6）发起一场促进网络安全公众意识的全国性教育运动。

（7）发展并完善政府对组建国际网络安全政策框架的观点与立场，加强与国际伙伴的关系，主动创新，解决所有与网络安全相关的问题。

（8）制定网络安全应急反应计划；启动旨在加强政府与民营企业伙伴关系的对话，理顺关系、加强协作，为扩大民营企业的参与并发挥其作用创造条件。

（9）与总统办事机构其他部门合作，制定一个研究和发展战略的框架，侧重于发展有助于提高数字基础设施安全性、可靠性、韧性和可信度的革命性技术；让研究界有权使用涉及重大事件的数据，以便开发手段，测试理论，并找出可行的解决办法。

（10）建立基于网络安全的身份管理构想和法律规定，以满足隐私和公民自由权利的关切，指导与加强隐私权保护的相关技术发展。

（二）中期行动建议

（1）对于有关法律解释、政策应用及网络操作权限的机构间的分歧，改进其解决的过程。

（2）使用管理和预算局项目评估框架来确保各部门机构在追求网络安全目标时使用基于绩效的预算编制。

（3）扩大对关键教育项目和研发的支持，以确保国家在信息时代的经济环境中保持持续的竞争能力。

（4）制定扩充与培训劳动力的战略，包括吸引并维持联邦政府内的网络安全专门技术人才。

（5）确定最高效、最有效的机制，以便获得战略性警报、保持态势感知能力和事故响应能力。

（6）制定一系列的威胁情景和指标，用于风险管理决策、恢复规划及研发的优先顺序确定。

（7）在政府和民营部门之间制定一项程序，以便协助防范、侦测并响应网络事故。

（8）建立网络安全相关的信息共享机制，消除有关隐私与专有信息的担忧并使信息共享具有互利性。

（9）制定相应的解决方案，要求在自然灾害、危机或冲突时期可以提供应急通信能力，同时确保网络的中立性。

（10）扩大与重要同盟之间有关网络事故和弱点的信息共享，并寻求双边和多边安排，这种安排将可以在提高经济与安全利益的同时，保护公民自由和隐私权。

（11）鼓励学术界和业界实验室之间的合作以便制定换代路径，以及鼓励快速采用研究与技术开发创新的刺激措施。

（12）利用基础设施目标和研发框架来帮助界定国家与国际标准制定机构的目标。

（13）对于高附加值的业务（如智能电网），建立一系列可以选择加入的、能够相互配合的身份管理系统，以便为在线交易建立信任并提高隐私水平。

（14）完善政府采购战略，并且对于具有韧性且安全的硬件与软件产品、新的安全创新及安全的托管服务，建立市场激励机制。

确保未来网络安全的蓝图：国土安全相关实体网络安全战略

一、部长致辞

我很高兴公布《确保未来网络安全的蓝图：国土安全相关实体网络安全战略》报告。该报告是根据《四年国土安全评估报告》要求公布的，反映了网络空间对我国经济、安全以及生活方式的重要性。

我们致力于建设的网络具有以下作用：推动创新和繁荣，推进经济利益和国家安全，并将保护个人公民自由、隐私权纳入美国国土安全部的网络活动当中。报告为打造这样的网络提供了蓝图。报告旨在保护对美国至关重要的关键基础设施，并在今后开发出更强大的信息和通信技术，使政府、企业和个人更安全地使用互联网。

维护网络安全人人有责，我们每个人都有责任在这方面发挥作用。网络安全威胁日益严峻，需要整个社会——包括政府执法部门、民营企业乃至公众参与维护网络安全。当前，美国面临多层次的网络安全威胁。构成网络安全威胁的主体既有黑客和有组织犯罪团体，也有拥有先进技术的国家。个人和组织严密的团体利用网络薄弱环节盗取美国的知识产权、个人信息及金融数据。网络窃密技术日益先进以及网络安全事件不断增多，对我们的经济竞争力构成了潜在威胁，并削弱了公众获得基本网络服务的能力。政府、非政府组织、民营部门乃至个人、家庭以及社区必须同心协力，有效减少网络安全风险。

州及地方政府、产业界、学术界、非政府组织及许多具有奉献精神的个人都为报告的撰写作出了贡献。他们的参与使国土安全部获益良多，在此谨致谢意。国土安全部还与联邦政府各个部门密切协同，完善这一报告，并确保报告与 2010 年《国家安全战略》、《网络空间行动战略》以及《网络空间国际战略》保持一致。

我还想感谢国土安全部各位同仁、成千上万的网络科学家、系统工程师、执法人员，以及为保护网络安全忘我工作的其他专业人员。我很高兴代表他们发布这份报告。

美国国土安全部部长　珍妮特·纳波利塔诺

二、执行概要

报告为建设可靠、安全及具有恢复能力的网络提供了一个明确方案。报告是在《四年国土安全评估报告》基础上撰写的。在该报告的指导下，美国各级政府、民营部门以及国际伙伴能够密切合作，增强维护网络安全的能力。这些能力对于我们的经济、国家安全以及公共卫生和安全至关重要。报告列出了两大行动领域：保护当前的关键信息基础设施和建设未来的网络生态系统。报告旨在保护最为关键的系统和资产，并推动人机协同方式的根本转变，以确保网络安全。在维护网络安全活动过程中，保护公民自由及隐私权是国土安全部的一项基本要求。

报告列出了保护关键信息基础设施的 4 项目标：

（1）减少网络安全风险；

（2）快速应对网络安全事件，提高网络恢复能力；

（3）共享网络安全信息；

（4）增强网络抗压能力。

报告将上述 4 项目标细化成 9 项具体目标。能否实现这 9 项目标取决于美国国土安全相关实体的能力建设情况，而这些能力在实际工作过程中将转化成具体措施。美国国土安全相关实体需要综合运用这些措施，以有效地预测和应对各种网络安全威胁。报告中介绍的一些措施在当前行之有效，而其他措施则需要进一步完善，还有一些措施需要进一步论证。为实现上述目标，有必要构建一个相互协作并能做出快速反应的网络安全社区。

报告还提出了加强网络生态系统建设的 4 项目标：

（1）提高个人和组织安全使用网络的能力；

（2）研发和应用更可信的网络协议、产品、服务、配置和架构；

（3）构建合作型网络社区；

（4）建立透明的安全流程。

报告将上述 4 项目标细化成 11 项具体目标。这些具体目标能否实现取决于报告中提到的一系列能力建设情况。

构建可靠、安全和具有恢复能力的网络环境的工作包括：评估网络安全能力建设的进展，确定这些能力能否有效应对不断演变的安全威胁。根据上述评估结果，我们将对每年的工作表现进行对比。这种方法将指出我们在能力建设方面的成绩和不足，明确下一步努力方向。

网络空间支撑着美国人生活的方方面面，并为美国经济、民用基础设施、公共安全及国家安全提供了重要支持。保护网络空间需要有远见、强有力的领导及国土安全相关实体所有成员的共同努力。美国国土安全部撰写这份报告的目的，就是探讨美国国家安全相关实体如何更好地确保网络安全。

三、引言

根据 2010 年《四年国土安全评估报告》制定的战略框架，国土安全相关实体实施行动的共同目标是确保美国本土的安全，并有能力抵御恐怖主义及其他危险。为实现这一目标，《四年国土安全评估报告》明确提出了 5 项核心任务，其中重点强调了网络安全对国家的重要性。

所有国土安全相关实体都有责任完成上述任务。来自各级政府、民营部门和非政府组织的个人都参与了上述任务。除国土安全部等正式肩负网络安全责任的机构外，每台计算机的所有者和关键基础设施的所有者及操作者都有责任维护网络安全。国土安全相关实体在维护网络安全过程中担负的责任和发挥的作用，反映出其规模庞大、丰富多样及相互依赖的特性。

《四年国土安全评估报告》将网络空间安全确定为核心任务的依据是总统发布的《国家安全战略》，该报告内容包括：

- 宣布数字基础设施是国家的战略资产；
- 将网络威胁视为最严重的国家安全、公共安全及经济挑战之一；
- 将数字基础设施的防护作为国家安全的重点。

国土安全部发布《确保未来网络安全的蓝图》的目的，是为国土安全相关实体落实《国

家安全战略》相关内容和实现《四年国土安全评估报告》提出的目标提供一套明确的行动计划：建立安全和有抗压能力的网络环境，推广网络安全知识和推进网络安全技术创新。

该报告的唯一指导原则是，在保护现有关键信息基础设施的同时，建设未来更为强大的网络生态系统。这一原则将指导资源的优化组合，从而系统地发展维护网络空间安全所需的各种能力。

（一）范围

2002 年《国土安全法》、第 7 号国土安全总统行政令、第 54 号国家安全总统行政令及 2002 年《联邦信息安全管理法》等文件指出，国土安全部在联邦各部门中负责牵头实施以下任务：保护联邦政府文职部门的信息和通信系统，与相关部门和企业合作保护关键基础设施，与各级政府合作保护其信息系统。“国家基础设施保护计划”、“国家快速反应框架”等文件描述了国土安全部及其他联邦政府部门在确认和保护国家关键基础设施中的作用。但联邦政府仅仅是国土安全相关实体中的一部分，该战略的成功需要相关各方的共同努力。尤其要指出的是，网络安全需要公共和民营部门在信息共享、创新、推广经验等领域展开强有力的双向合作。

从上述内容看，本报告旨在向国土安全相关实体提供实际和有意义的指导，使其能够确保网络空间的安全，并使所有希望能安全使用信息及通信技术的人受益。

（二）与其他重要政策和战略的关系

本报告支持以“政府一盘棋”的方式维护国家安全，并在制定过程中充分考虑了当前的国家网络空间战略和政策，其中包括：《网络空间政策评估》、《网络空间国际战略》、《打击跨国有组织犯罪战略》、《综合国家网络安全倡议》、第 7 号国土安全总统行政令、第 54 号国家安全总统行政令、《网络空间可信任身份国家战略》及《国防部网络空间行动战略》。

（三）动机

美国高度依赖网络空间。网络空间是现代社会的支柱之一。但网络技术在丰富我们的专业和个人生活的同时，也给一些人提供了扰乱或破坏我们生活方式的能力。保卫和控制网络空间隶属国土安全工作的范畴，是因为可能导致严重后果的大规模网络事件将损害公共和私有部门的重要功能与服务，影响我们的国家安全、经济活力及公共健康和安全。

由于恶意使用网络者正在使用越来越复杂的手段、技术及程序，网络事件的数量和复杂程度不断上升。

关键基础设施必须能够抵御复杂和持续的破坏行动，并做好应对更多破坏性攻击的准备。这种破坏行动会削弱或扰乱我们所依赖的基本服务。

政府机构必须防备可能移除或损毁敏感数据并干扰重要服务的非法行为。

大型企业、小企业和非营利组织面临着技术日益复杂的入侵行为，其对象主要是上述机构的消费者和客户的知识产权及个人信息。

消费者面临的风险通常是个人信息被盗，入侵者主要通过互联网上无数的站点实施未经授权的入侵行为。

（四）战略预想

尽管我们无法预测未来网络空间的具体情形，但我们必须制定一套充分掌握正在塑造未来网络空间的各种力量要素的相关战略，以确保美国拥有在网络空间中的领导、影响和应变能力。因此，该战略应建立在以下预想之上。

恶意网络行为的数量和复杂程度的不断提升，要求我们共享网络安全信息，快速应对网络安全事件，打造一支专业的网络安全人才队伍。

社会、经济和产业领域对信息和通信技术的依赖不断加深，不仅有助于提高生产力和促进创新，而且增加了网络用户群、扩展了网络技术设施以及需要保护的网络路径。

网络发达的互通性使其超越了地理边界，为国际合作提供了极大便利。但其存在的风险也从根本上改变了美国安全威胁的构成，这就要求我们调整现有的安全和威慑机制。

随着网络数据信息的急剧膨胀，分散和远程的网络管理既提供了新的机遇，也带来了更多的安全挑战。移动技术的发展使入侵者更容易获得敏感信息。网络风险的差异和个人、机构等对网络安全等级要求的不同，使以往“一刀切”式的安全防护措施不再有效。相关部门应制定一套基于风险的应对方案，使之能够随时进行调整、重点关注网络输出和运行情况、提高用户应对能力、促进创新和符合投入产出比原则。

信息和通信技术供应链的全球化为促进创新和鼓励竞争提供了机遇，同时也带来了更多风险。

四、我们所追求的未来

信息革命几乎改变了我们日常生活的方方面面。可靠的数字化基础设施将为创新和经济繁荣提供一个持续的平台，并使我们能够在遵循我们核心价值观的情况下，推进美国的经济和安全利益。为使我们的下一代发挥出信息革命的全部潜力，国土安全相关实体必须确保建立可靠、安全和具有抗压能力的网络空间，同时提升网络安全意识和创新能力。这一复杂而高强度的行动需要大量研发投入并经过实践的检验。本报告将为此提供强有力的基础。

根据《四年国土安全评估报告》的相关要求，国土安全相关实体应致力于实现以下目标。

（一）一个安全的网络空间

为了保护美国及其民众、核心利益和生活方式的未来，我们将在确保网络空间安全方面取得重大进展。国防和创新领域的敏感信息将得到进一步保护。美国民众在进行网上交易时将更有信心，影响关键信息基础设施的安全风险将被降至最低。个人和机构将具有较强的网络安全意识，并能采取相应的安全措施。美国国内及国际网络安全政策、法规将能及时反映当前的网络环境状况，并预见到未来的安全需求。监管机构拥有必要的网络工具和人才队伍，以确保各机构落实相应的安全措施。各国成为负责任的网络空间行为主体，并拒绝为恶意使用网络者提供“庇护所”。一旦网络空间被恶意利用，各机构能使用必要的手段锁定入侵者并将其绳之以法。联邦机构和民营领域实体将拥有必要的网络安全专业技术人员，以满足其任务需求。

（二）一个具有抗压能力的网络空间

提升个人、社区网络系统的活力、适应能力、快速反应能力和修复能力。未来，我们打造

的网络安全框架将能实时侦测网络威胁，并根据不同的突发事件制定相应的信息防护措施。包括通过模拟、仿真和演习，来确认和降低安全威胁等级。演习能定期检验关键基础设施的快速反应能力和计划的可持续性，并为决策者和投资者提供对策建议。国土安全相关实体将拥有灵活的信息分享机制——关于威胁、弱点和防护能力的重要内容将在公共和民营部门进行实时传输。在网络安全关键行动继续展开的同时，网络安全框架也将对重大事件做出快速反应。

（三）一个鼓励创新的网络空间

通过合作创新，实现人、设施和市场的互连，以促进经济增长。未来，美国人将拥有无处不在的网络接入设施。它将使个人、企业和市场之间的互联互通更加迅速和便捷。随着互联网用户使用新的网络设备，以往各自隔离的实体之间的交流将越来越多。新的信息和通信技术将把新兴市场与发达市场连接起来，并随着信息的加速流动，推动跨地区合作和促进欠发达地区的经济增长。以往的单机装置，如能源仪表和家用电器，将越来越具有通用性，消费者和企业将从中受益。更具活力的安全机制将降低消费者的风险，并使各机构获得更优质的服务和安全防护能力。在确保网络空间安全的同时，我们还要维护自由贸易原则、促进更大范围信息的自由流通、承担全球责任以及满足国家的需求。

（四）一个保护公共健康和安全的网络空间

确保美国民众的安全。未来，管控能源、交通运输、化工和关键制造业等关键基础设施部门的工业系统和控制系统，以及运行在各类医疗设备、交通工具和其他领域中的嵌入式系统，均能更好地抵御各类可能危害公共安全的网络破坏和攻击行为。在这一网络空间中，执法和应急反应等重要公共安全部门也能继续依赖完整且随时可以使用的信息和通信技术。

（五）一个促进经济利益和国家安全的网络空间

增强美国的经济竞争力和国防安全。未来，安全、可靠的网络空间将为美国经济增加动力，使美国继续保持经济强国地位。在该网络空间中，商业部门将更加充分地了解其面临的风险，对其知识产权的保密性、完整性和可用性也将充满信心。安全的网络空间能够支持国民经济有效运行，也可支持各类关键社会服务的开展。健康的网络空间还有利于国土安全部完成其他任务：预防恐怖主义，维护边境安全，执行移民法，以及从事故灾难中迅速恢复。最后，通过同美国国防部合作，这一安全的网络空间将支持美国政府履行其保护国家安全的关键使命。

五、指导原则

美国人的价值观、基本原则和生活方式为报告提供了指导原则，其基础是保护隐私和公民自由。报告也体现了美国提出的“开放政府倡议”中的透明、参与和协作等理念。开放使民主变得更为强大，也可使政府的效能与效率得到提升。坚持上述原则是各利益攸关方增强本报告所述各种能力的关键。

（一）隐私和公民自由

在确保网络空间安全的过程中，国土安全相关实体将保护公民权利和尊重隐私。每个公

民都可了解其个人数据将如何被使用，并可相信其使用是恰当的。美国国土安全相关实体将支持一个开放、互动的网络空间，个人可借此在全球范围内寻找、接受和影响各种信息和思想。信息的自由流动是互联网快速演变和成长的关键所在。网络空间也必须继续成为自由连接和自由表达的场所。

（二）透明的安全流程

国土安全相关实体将在高度透明和负责任的流程下开展保护网络空间安全的活动。坚持“按需分享”和“谁提供谁负责”的合作原则，将使具体、可操作的网络安全信息得以传送给需要的人员，同时保护公民自由和隐私。美国政府、民营部门和国际伙伴之间的互动，可增进安全措施的效能，并提升决策质量。这既兼顾了公私利益，又有助于共享网络安全信息。

（三）在分布式环境中共担责任

保护网络空间安全的各种力量散布在国土安全相关实体中，大量的网络安全专家也分布在诸多不同领域。因此，国土安全相关实体将利用网络空间这一分散性来保护网络自身。国土安全相关实体将继续努力增强地方政府和个人的能力，通过集体行动汇聚所有力量，以实现共同的安全利益。为确保所有人都处于安全的网络空间环境中，每个人都必须承担责任。国土安全相关实体将培养共同的责任感和公民义务意识，也将综合运用各种知识来处理安全问题和开展网络空间安全行动。

（四）基于风险、费效比高且便于应用的安全政策措施

在个人、机构和国家等层面，网络空间的安全风险和对这些风险的承受能力各不相同。在确定网络空间中的关键系统及资产和必须应对的最主要风险的过程中，国土安全相关实体必须与他们分享见解。国土安全相关实体将区分网络空间安全行动的轻重缓急，以确保将资源持续地用于可最大程度降低风险的领域。有效降低网络空间的脆弱性，有赖于全面系统地评估各种网络空间安全政策措施的风险、成本和应用情况。在使用信息和通信技术的过程中，所有用户都面临某些风险。必须更好地了解这些风险，才能在参与网络活动和交流时做出明智的决定。

六、战略概念

报告体现的唯一且一致的战略概念是，在保护现有关键信息基础设施的同时，建设未来更为强大的网络生态系统。这一战略概念将指导美国建立安全、可靠及具备抗压能力的网络空间，并形成各利益攸关方共同致力于提升美国网络空间能力的局面。

（一）重点关注领域

该战略概念包含两个互为补充的重点关注领域

（1）保护关键信息基础设施。重点关注网络生态系统中的软、硬件设施对美国至关重要。减少信息基础设施面临的威胁，确保其具备快速反应能力和网络安全信息共享能力，以及增强其快速恢复能力是保护信息基础设施的最佳途径。

（2）提升网络生态系统的能力。此举旨在推动人机协同方式发生彻底变化，使人与设备

能够更好地“融合”，以此确保网络空间的安全。这一革命性的改变将通过提高个人维护网络安全的能力，研发和使用更为可靠的网络协议、服务和产品，加强相关部门在维护网络安全方面的协作，以及建立透明的工作流程等方式实现。

（二）成功的含义

国土安全相关实体的投入产出效益将通过量化的标准加以衡量。

1. 保护关键信息

基础设施在面临最严峻的威胁时，基于效果的衡量标准如果能够证实关键信息基础设施的所有者和经营者能够妥善管理风险，信息基础设施能够确保安全，即认为关键信息基础设施得到了切实有效的保护。

2. 建设网络生态系统

当符合下列条件时，网络生态系统才是安全的。

（1）用户能够充分认清、掌握和管理信息和通信技术风险。

（2）机构和个人能够按规定执行安全和隐私保护相关法规。

（3）个人、机构、网络、服务和设备满足网络安全标准。

（4）信息和通信技术具备安全的通用性。

（5）接近实时的端对端协作能够对网络安全事件发出警告并自动做出反应。

（三）如何保护关键信息基础设施

确保国家关键信息基础设施的安全，需要联邦政府各个部门和机构之间的多边合作，也需要联邦政府、州和地方政府、非政府组织和民营部门之间的业务合作。在联邦政府层面，国土安全部与军队、情报部门和执法部门的协作是我们防范和有效应对网络威胁的基础。报告描述了国土安全部如何根据第 7 号国土安全总统行政令、第 54 号国家安全总统行政令及 2002 年《联邦信息安全管理法》，与合作伙伴共同采取防范措施。国土安全部将发挥坚强的领导作用，保护联邦政府中非保密的文职部门。

报告列出了保护关键信息基础设施的 4 项目标，国土安全部将采取 9 项措施实现上述目标。实施过程中，各种措施需要相互配合以有效地预测和应对各种威胁。其中一些措施在当前行之有效，而其他一些措施则需要进一步完善，还有一些措施需要进一步论证。为实现上述目标，有必要建立一个相互协作且能做出快速反应的网络安全社区。

每种能力都包含相应的人员、流程和技术因素。由于网络社会具有全球性，我们需要与国际伙伴共同建设和运用这些能力。报告的结语部分将详细介绍如何在后续的实施计划中对能力进行优化组合。

美国国土安全部支持通过新的立法，以促进在政府和民营部门之间自愿分享合法获取的网络安全信息。此外，相关立法行动应在现有指导原则之下，为民营部门分享网络安全信息提供免责保护。相关法案还应鼓励政府和民营部门以适当方式及时分享网络安全信息。

网络安全立法活动应在透明和充分吸收广大民众意见的基础上授予或加强国土安全部以下权力。

- 为加强网络安全，确定拥有或负责运行关键信息基础设施的实体。

- 确定需要应对的具体网络安全风险。
- 评估并确定应对上述风险的标准化程序。
- 要求相关实体完善维护网络安全的计划，确定应对上述网络安全风险的方法。
- 建立第三方评估机制，评估相关实体在管理和应对网络安全风险方面的效能。

国土安全部支持通过修正《联邦信息安全管理法》，使国土安全部担负起联邦文职行政部门信息安全的主要责任，这将赋予国土安全部以下权力。

- 公布必须执行的信息安全政策和命令。
- 评估相关机构的信息安全计划。
- 指定相关实体负责接收信息安全方面的报告，内容包括信息安全事件、威胁及影响信息系统的弱点等。

1. 减少网络安全风险

1）规避威胁

通过持续运用国土安全部国家网络安全保护系统，削弱国内外罪犯利用、损害、瘫痪或摧毁关键信息基础设施的能力。

国土安全相关实体应具备的核心能力包括以下几方面。

- 防入侵系统及其他安全技术。这可减少进出信息和通信系统的恶意流量。
- 在防止、调查和起诉网络犯罪行为过程中加大国内法和国际法的执法力度。
- 通过专门的技术训练、使用先进的调查手段、建立相关国际合作等方式，加强证据共享及将犯罪分子绳之以法的能力。
- 通过全源信息搜集和分析，确认相关威胁的实施者及其使用的策略、技术和步骤。
- 就关键信息基础设施面临的最严重威胁发布及时、有针对性和可操作性的信息。信息共享论坛、分析中心、工作小组、提供合作的门户网站、简报及其他机制的运行，有利于国土安全相关实体中的利益攸关方进行威胁信息的分发和交换。
- 组建与威胁信息的发布者和使用者进行接触的团体，从而确立描述、解读和自动处理威胁信息的标准。
- 将网络安全事件报告的指导方针和激励措施发放至适当的机构和个人，包括网络安全专家和各级政府，以及联邦执法部门和突发事件反应中心。

2）强化关键信息基础设施

采用适当的安全措施以管理关键系统和资产面临的风险。

国土安全相关实体应具备的核心能力包括以下几方面。

- 确定在受到干扰、破坏或毁坏的情况下，最有可能对国家安全、经济安全和公共健康或安全造成影响的关键信息基础设施，其中包括网络互连节点、域名系统、卫星地面站、电缆平台、工业和监控系统、关键商业或交通系统和其他支持关键功能和服务的系统。
- 运用技术和相关指导原则对网络进行管理。
- 评估各类网络威胁并根据结果确定重点领域，如某个特定的威胁会利用网络的脆弱性并引发严重的后果。在系统、组织、部门、区域、国家和国际层面的威胁评估将帮助公共和民营部门的相关实体了解其面临的风险，从而使其能确定优先行动领域

以降低风险和进行投资。

- 借助相关网络安全标准有效应对威胁。运用具体的管理手段、技术和安保措施以降低风险，这已被写入联邦政府文件当中。
- 不间断地对内部网络进行监督和测定，确保风险管理根据技术或风险环境的变化实时进行调整。对风险管理的第三方评估将验证该行动是否符合标准。

上述措施将对关键基础设施的技术弱点进行界定、分类，并找出需要关注的重点领域。

3）实现革新

寻找新方法以应对业已存在的问题，同时开发应对潜在安全挑战的新技术。

国土安全相关实体应具备的核心能力包括以下几方面。

- 将研发重点放在需要优先考虑的关键安全领域。联邦网络和信息技术研究与开发计划列出了以下研究重点：“内置式安全措施”、“定制可信的网络空间”、“移动目标”及“网络经济激励措施”。
- 迅速应用新开发的产品和工具，以应对不断变化的网络安全威胁。
- 整合国家网络研发活动，包括国防、执法、反谍报部门等开展的研究活动。

2. 快速应对网络安全事件、提高网络恢复能力

1）鼓励相关实体优先采取行动

重大网络安全事件威胁公共安全，削弱公众信心，影响国民经济和国家安全。因此，一旦发生重大网络安全事件，相关实体应采取联合行动，迅速做出反应，恢复网络安全。

国土安全相关实体应具备的核心能力包括以下几方面。

- 及时和准确查明、报告、分析网络安全事件并做出反应的能力。当网络安全事件发生时，应通过国家网络安全和通信中心等负责监视和预警的部门，协调有关部门，搜集与汇总网络安全事件的信息，协调联邦、州、地方政府部门以及民营机构和国际伙伴的行动，以及时和准确地查明、报告、分析网络安全事件并做出反应。
- 制定成熟和操作性强的应对和恢复预案的能力。该预案不仅能应对网络安全事件造成的物理性后果，还要能消除物理破坏造成的网络影响。
- 建立强大伙伴关系的能力。为了迅速重建关键信息基础设施，国土安全相关实体需要建立强大的伙伴关系，包括与第一批做出反应的相关实体密切合作，以及在必要时政府或民营部门的专家提供远程或现场技术帮助。
- 网络威胁调查和分析能力。通过网络威胁调查和分析，确定恶意网络行为对基础设施的影响。通过提供法律行动所需的证据，为采取反制措施提供前瞻性分析，预测和防范未来可能发生的敌意行为。联邦调查局领导的国家网络调查联合特别工作组就是专门从事网络威胁调查和分析的跨部门机构，它具有扭转攻击造成的被动局面、确定攻击者的数字和物理特征等能力。
- 标准化的自动修复能力。将系统恢复至正常、安全的状态。

2）做好网络突发事件应急准备

举行网络安全演习，以检验应急计划并总结经验教训。

国土安全相关实体应具备的核心能力包括以下几方面。

- 组织跨部门演习的能力。评估和验证各个部门在信息共享、事件反应和恢复等方面

的准备情况。

- 组织在特定机构和部门内部举行演习的能力。在系统、组织、机构、地区、国家和国际等各种层面，检验其应对网络事件并从中恢复所需的步骤、程序、报告机制等。
- 整体规划能力。运用商业网站、与软硬件和网络服务供应商达成协议等手段，并综合考虑设施、人员、装备、软件、数据文件和系统构件的基本情况，进行整体规划。
- 建立相关机制的能力。该机制应包括对演习进行评估、总结经验教训和制定改进计划等内容。

3. 共享网络安全信息

共享网络安全信息是减少网络安全风险、快速应对网络事件和提高自我恢复能力的关键。

1）整合信息

对从不同机构、地域、国家和国际资源中获得的信息进行整理、归纳。

国土安全相关实体应具备的核心能力包括以下几方面。

- 国家网络安全防护系统。该系统由人和传感器组成，可根据特定网络安全相关实体的需要搜集并实时交换信息，这些信息主要涉及网络威胁、弱点、后果、预警和反制措施的信息。
- 分析能力。迅速分析不同来源的相关信息，帮助各级决策者和网络安全设施防止恶意网络行为。为此，国土安全部应与其他联邦机构合作，向国土安全相关实体提供无差别的、有用的网络安全信息。
- 与可信赖的伙伴共享信息。这些伙伴包括同类和相互依赖的组织、政府机构和企业，将它们联系在一起的机构是降低风险联合中心、特定部门信息共享和分析中心、部门协调委员会、安全和网络行动中心、计算机事件反应小组。
- 建立统一的标准。按照预定程序收集和存取信息，根据相关协议或谅解备忘录、部门间协议等建立可信的信息共享环境；签署协议和建立国家层级的机制，如保护关键基础设施信息项目的信息标识，以保护民营机构与联邦政府所共享的信息。

2）有效分发信息

利用多种平台及时发布特定的行动性信息。

国土安全相关实体应具备的核心能力包括以下几方面。

- 及时交换网络预警信息。美国政府与各利益攸关方通过以下平台交换网络预警信息，如美国计算机应急小组预警系统、国防部网络态势预警系统、联邦调查局初级防护项目、美国特勤局电子犯罪特别小组、国家标准和技术数据研究所等。
- 建立强大的信息分发平台。该平台无论在平时，还是在发生重大网络事件时，均能向各利益攸关方持续分发网络威胁的特征、标识、弱点等信息，并提供应对威胁的具体方案。
- 有效的沟通战略。利用社会媒体进行沟通时，应努力确保时效性与沟通频率，保持沟通顺畅并能控制相关风险。
- 可方便使用数据信息的措施。在必要时或向更多公众提供信息时，该措施能保护信息来源、传播途径和平台安全。

- 采取经济激励等措施。通过赠予、补贴、税收优惠以及提供可靠的保护措施等手段来促进合作。

3）为网络从业人员提供专门的网络安全培训和认证

培训网络从业人员以提高其竞争力。

国土安全相关实体应具备的核心能力包括以下几方面。

- 改进培训方法。使网络技术人员能够设计、建立安全且具有恢复能力的信息技术系统。
- 做网络安全专业知识的提供者。这种知识能够通过课堂或其他类似环境下的学习，以及在公共与民营部门之间进行人员轮岗的方式来获得。
- 发展并运用网络安全相关职业与领域的“成熟能力模式”。这些职业与领域包括信息技术管理、电子工程、计算机工程和通信业。“成熟能力模式”用来描述在初、中、高三种等级从事特定任务所必需的技术能力。

4. 增强网络抗压能力

提高网络的纠错能力。增强系统在网络安全环境恶化的情况下完成核心任务的能力。

国土安全相关实体应具备的核心能力包括以下几方面。

- 全面理解关键基础设施存在的弱点和可能导致系统崩溃的潜在漏洞。
- 设立结构性指导原则和恢复能力标准。例如，减少多路通信过程中可能出现的单点阻塞，在正常状态下快速存储，出现错误时立即实行隔离并遏制扩散，建立恢复模式以最大限度减少损失。
- 与现有恢复能力标准和指导原则保持一致，包括符合美国国家标准与技术研究所出版的《信息技术系统的应急计划指导》、国际标准化与国际电子技术委员会颁布的《信息技术安全技能：信息与通信技术长期规划指针》的相关要求。
- 根据“网络与信息技术研究发展项目”，掌握在软件和网络方面自主创新的方法。
- 持续评估确保恢复能力的战略与项目的效果。

（四）如何建设网络生态系统

如上文所说的“智能电网”一样，关键信息基础设施是网络生态系统的一部分。国土安全相关实体将在维护网络生态系统安全性方面取得阶段性进展。这需要我们增强个人与组织安全使用网络的能力，开发和使用值得信赖的协议、产品、服务、配置及架构，建设合作型网络社区以及确保进程透明。为加强网络生态系统建设，本报告提出以下 4 项目标以及 11 项具体目标。

1. 增强个人和组织安全使用网络的能力

1）增加公共与民营部门的网络从业人员

维持一支强大的网络安全专业队伍，其工作是开发和应用网络安全技术，以确保消除当前及未来的威胁。

国土安全相关实体应具备的核心能力包括以下几方面。

- 发展一套严格的网络安全与软件学习课程，以保证能持续学习特殊领域的专业知识。相关科目应涉及科学、技术、工程及数学。美国国家网络安全教育机构将推出

正式的网络安全教育项目，通过设立从幼儿园开始的 12 级技能培训、更高等级的教育与职业项目等方式，提高相关人员的技术水平。此外，四年制及有资格授予研究生学位的大学应成为美国信息技术教育方面的学术研究中心。

- 通过提供奖学金、补贴及税务优惠等措施鼓励学生学习特定领域的专业知识。“联邦网络服务：公共事业项目奖学金”将向那些进入特定机构进行深入学习的学生提供奖学金，以资助其在书本、学费及住宿等方面的开支。
- 拴心留人。保留人才可通过以下方式进行：积极招募、快速录用、破格提拔、在职培训，以及开展雇员满意程度调查。
- 具备必要技能。包括视情颁发网络安全专业合格证书。

2）为分布式安全建立基础

向个人提供与其身份相符的资源，如工具、建议、教育、培训等，使其能依据当前网络安全特性及协议、产品与服务情况维护各自网络安全。

国土安全相关实体应具备的核心能力包括以下几方面。

- 在国家、社区及机构三个层面开展网络安全活动，为特定人群提供建议、资源、工具，帮助其理解网络安全威胁，并在加强网络生态系统建设方面发挥各自作用。这些活动在联邦、州、市、县、印第安人保留地及海外领土等各个层级展开，包括国土安全部的“停一停、想一想、再上网”活动、“国家网络安全意识月”等。
- 为个人采取网络安全措施提供最佳行动指导。
- 建立一套机制，提醒用户其使用的工具和系统存在漏洞或已被感染，并使用户能据此采取行动。

2. 开发并使用可信的网络协议、产品、服务、配置与架构

1）降低脆弱性

开发并应用专门用于减少漏洞的信息与通信技术，该技术能通过维持或强化系统安全态势，及时感知、应对及输送系统内部及周边系统安全态势所出现的变化。

国土安全相关实体应具备的核心能力包括以下几方面。

- 在那些有权设立国际标准的组织和论坛中保持领导地位。
- 推广使用安全的软硬件产品。
- 树立贯穿于系统开发整个周期的安全意识。
- 建立安全产品的评估与认证制度。
- 增强开发技术、拟定标准的研究能力。
- 改革商业市场，缩短新技术应用周期，以应对不断出现的网络威胁。
- 整合供应链，提高值得信赖的产品与服务的应用效率。

2）提高可用性

开发可信的技术，使之易于使用、易于管理，并能快速定制，发挥预期的效能。

国土安全相关部门应具备的核心能力包括以下几方面。

- 提出需求和指导纲领，以阐明在部件组装、体系构造、运行管理、人机界面和可用性网络性能方面的主要特点。人机界面的标准由美国国家标准协会发布，而可用性网络标准是由欧盟发起制定的。

- 研究并确定有关用户社区内那些可被迅速采纳和标准化的安全技术，并使之融入研发进程。

3. 建设合作型网络社区

国土安全部白皮书《强化网络空间的分布式安全》提出了认证、兼容和自动控制三种能力。

1）网络身份认证

采取基于风险的原则进行认证，提高参与网上信息交换的个人和机构的网络身份信任等级。

国土安全相关实体应具备的核心能力包括以下几方面。

- 基于风险和敏感活动的认证和授权。
- 采取加密登录、数字证书和其他多种认证方法，以降低敏感信息交换的风险。
- 加强网络管理，包括改进体系设计、基于用户的设计、基于政策的邮件路由和储备、确保内部关联和避免相互干扰、提高系统兼容性以及管理方法。

2）提高各技术设备之间的技术和政策兼容水平

在设备对设备层级，加强合作，促进创新，增强网络安全信息共享能力。

国土安全相关实体应具备的核心能力包括以下几方面。

- 具备网络突发事件的预警能力。该工作借助有关重要信息要素的标准化参考文件展开，内容包括确认软件脆弱性、薄弱环节、网络攻击范式、恶意软件分类以及传输的安全内容，而后者是依据自动分享原则设置的。其信息来源包括“国家脆弱目标信息库”、“普通脆弱性和暴露性目标（信息库）”，以及属于“国家检验清单项目”的“信息确保清单”。
- 建立统一的界面标准，以使诸如公共关键密码系统标准、无线电频率识别器空中界面标准和数据格式标准能够实现技术兼容，实现辨别指纹、面部和其他生物特征信息。

3）自动化安全步骤

以接近实时反应的方式，通过自动化机制，预测和防止攻击事件，缩小事件在联网各设备之间的传播，将事件危害降至最低水平。

采取数字化政策，使所有者和用户能够采取可靠的安全行动，按照有关政策，将遭受病毒感染的设备脱离网络连接。经批准后，改变未受病毒感染设备的配置，使其更加强健，以应对网络入侵，并防止恶意软件攻击和未经授权的网络信息外流。

确立合作框架和程度，建立一致的网络安全目标、共同行动原则，从而提高反应速度，优化决策程序，以便采取新的安全措施。

4. 建立透明的安全流程

1）公布网络空间的突发事件及原因

像卫生官员向公众通报健康和疾病信息一样，向公众提供翔实的网络空间安全威胁信息，核实当前和未来网络地址（如.gov、.com 和.edu）中攻击事件发生的位置，了解其原因、范围和影响。

国土安全相关实体应具备的核心能力包括以下几方面。

- 设立信息共享机制，以使匿名化传输的事件数据能被当前事件监管部门兼容使用。
- 向国土安全相关实体和国际伙伴分发有关网络安全能力、态势、危险和事件爆发的信息，以使有关各方能自动采取预防措施。
- 与国防和情报界合作侦测网络威胁。

2）基于效果采取安全举措

同有关各方分享有关网络协议、产品、服务、配置、设计、供应链和组织流程的安全绩效信息。

国土安全相关实体应具备的核心能力包括以下几方面。

- 向国土安全相关实体和国际伙伴分发有关网络协议、产品、服务、配置、设计、供应链和组织流程的安全绩效信息，以遏制网络危险的传播和影响。
- 建立机制，优先向基于效果和能力的项目投资。这种效果和能力应被证明能将风险减至可接受的水平。

3）关注投资回报

评估网络安全投资对组织机构的影响，集中于运行成本、基本建设预算、业务灵活性，以及因数据侵权或未能履行服务协议而支付的赔偿支出。

国土安全相关实体应具备的核心能力包括以下几方面。

- 通过使用量化网络安全投入和迅速确立投入产出比的方法，加快采取和执行网络安全措施的速度。
- 维护并共享数据，以便论证网络安全的投入产出效率。

4）激励履行职责

建立、维护并提高有关网络安全的目标和措施体系。

国土安全相关实体应具备的核心能力包括以下几方面。

- 设定希望达成的目标和成果并积极采取行动，以使国土安全相关实体能明确其任务要求。
- 提出支持国土安全相关各方目标的需求、指导原则、政策方针、步骤流程和自愿性的行动守则。
- 建立相关程序和机制，评估检验其获得的进展。
- 分析网络安全措施、项目和计划的成效和影响，如发现不足，应努力重新设定目标，并不断取得进步。

七、结语

网络空间支撑着美国生活的方方面面，并为美国经济、民用基础设施、公共安全及国家安全提供了重要的支持。保护网络空间需要有远见、强有力的领导及国土安全相关实体所有成员的共同努力。这种努力预见和增强了团队协作、相互负责、认可与支持的文化。

这一战略明确阐述了实现国家安全战略构想及《四年国土安全评估报告》目标的方式，即建立可靠、安全和具有恢复能力的网络环境，推广网络安全知识和创新。“保护关键信息基础设施”和“加强网络生态系统”两大任务重点将促进国土安全相关实体的能力、行动及资源的优化组合。在国土安全部，这一进程将有助于制定为期五年的“未来国土安全项目”。

国土安全部将与国土安全相关实体中的利益攸关方合作，共同制定一份能够合理安排行动、设定关键转折点和跟踪进程的实施计划，用以建设该战略所需的各种能力。此外，国土安全部将带领国土安全相关实体制定相关标准，用以衡量关键安全能力的有效性。国土安全部还将在国土安全相关实体内部设立相关基线，从而能将每年的成绩与上一年进行比较。这一行动将重点突出取得的成绩、存在的问题及额外需要的资源。为满足遂行网络安全任务的需要，国土安全部将继续根据相关法律和原则保护隐私及公民权利。

保护网络空间是一项要求所有人都积极参与的复杂事业。通过利用这一报告提供的框架，我们将为实现我们的目标而努力进取。通过上述努力，国土安全相关实体能使网络空间成为推动美国生活方式繁荣永续的安全之所。

总 统 令 篇

克林顿政府关于关键基础设施保护的白皮书

这份白皮书阐述了克林顿政府关键基础设施保护政策的核心要素，将适用于包括公共和民营部门的所有利益相关方，也将用于如国防大学和国家外交事务培训中心等美国政府职业教育机构以指导跨部门的课程及训练。这份公开白皮书的广泛传播得到了所有美国政府机构的支持。

一、日益增加的潜在漏洞

美国的经济实力和军事实力在全球首屈一指，这两方面是相辅相成的，并且越来越依赖特定的关键基础设施和网络信息系统。

关键基础设施是指完成经济和政府行为必需的基本物理网络系统和资产，主要包括政府和民营部门的通信、能源、银行和金融、交通、供水系统，以及应急服务系统。以前，这些关键基础设施无论在物理上还是逻辑上都是相互独立、互不依存的。然而，随着信息技术的发展以及提高效率的需要，这些基础设施的自动化程度日益提高并相互关联。这些进步也带来了新的漏洞（设备失灵、人为失误、天气、自然灾害，以及物理或网络攻击）。因此，我们需要公共部门和民营部门共同采取灵活先进的方法来保护国内外安全。

由于军事实力强大，未来的敌人，包括国家、组织或者个人，将会寻求用非传统的方式对美国发起攻击，包括在美国境内的攻击。美国的经济越来越依赖于相互依存的以网络为支撑的基础设施，对我们的基础设施和信息系统的非传统攻击将严重危害到我们的军事力量和经济发展。

二、总统的计划

长期以来，确保关键基础设施的连续性和可用性一直是美国国策。克林顿总统计划，美国将采取一切必要措施迅速消除任何可对关键基础设施发起物理或网络攻击的重大漏洞，特别是攻击网络系统的漏洞。

三、国家目标

2000 年之前，美国应当实现初步的信息保障能力；从此总统令发布之日起 5 年内，美国要具备并维持使我国的关键基础设施不被蓄意攻击的能力，以免造成以下国家能力的显著降低。

- 联邦政府履行必要的国家安全职责，以保障普通公民的健康和安全。
- 州和地方政府维持治安并提供最基本的公共服务。

- 民营部门确保经济的有效运转并提供必备的通信、能源、金融和交通服务。

这些关键性政府功能的任何中断或恢复运行必须是短期的、不频繁的、可控的、在地理上孤立且对美国利益损害最小化。

四、建立政府与民间的合作关系以减少漏洞

由于经济部门和政府的关键基础设施极易成为攻击目标，因此，消除潜在漏洞需要政府与民间部门紧密配合，共同努力，相互信赖，相互合作。为了消除关键基础设施的漏洞，应该（并且是合理可行的）避免政府加大监管力度，或未备基金的政府部门过度干涉民营部门。

对于每一个可导致主要经济行业的基础设施受攻击的漏洞，联邦政府都将从主管部门委派一名高级政府官员作为部门联络员，与民营部门开展合作。部门联络员经过与该行业民营部门的讨论与协作，在民营部门确定一名相应人员，即部门协调员，代表该行业。

此二人与其所代表的行业共同通过以下举措为该行业的国家基础设施保障计划作贡献。

- 评估该行业可能受网络或物理攻击的漏洞。
- 制定消除重大漏洞的计划。
- 建立识别并预防重大攻击的系统。
- 制定计划，预警并阻截正在发生的攻击，并在美国联邦应急管理署（FEMA）的帮助下，在遭受攻击后快速恢复最低限度的基本能力。

在这一保障计划的筹备阶段，国家协调员应与政府的部门联络员以及国家经济委员会的一名代表共同确保各部门计划的整体协调和整合，要特别关注各部门的相互联系。

五、指南

为消除潜在漏洞，克林顿总统考虑到以下通用原则及关注点。

- 我们将商讨并寻求符合国会规定的方法和程序，以实现该指令设定的目标。
- 保护关键基础设施需要所有者、经营者和政府共同承担责任，建立伙伴关系。此外，联邦政府还将鼓励国际合作以帮助管理日益增长的全球问题。
- 由于威胁关键基础设施的技术和特点发展迅速，应该对关键基础设施的当前可靠性、脆弱性和威胁环境进行频繁评估，因此，我们的保护响应和措施必须具有很强的适应性。
- 市场激励机制是实现关键基础设施保护的首选。只有在市场手段未能保护美国公民的健康、安全和福利时，才采取监管措施。在这种情况下，政府机构将确定和评估可以采用哪种备用方案进行直接监管，包括采用经济刺激鼓励期望行为，或者通过民营部门提供可供选择的信息。这些激励措施以及其他举措，旨在促进采用最新技术，使用全球化的解决方法应对国际化问题，并使民营部门的所有者和运营商拥有并保持最佳的切实可行的安保措施。
- 政府所有的权力、能力和资源，包括执法、监管、外交情报和国防都可适当使用，以确保并维持对关键基础设施的保护。
- 必须尊重隐私权。消费者和运营商都必须相信信息处理是准确、保密、可靠的。
- 联邦政府应进行研究、开发和生产，并鼓励引进越来越多的能够保护基础设施的方法。

- 联邦政府应为民营部门提供一个模型，确保基础设施达到最佳、合理且可行的状态，以完成其应尽的功能。
- 我们必须关注预防措施和危机管理。为此，应鼓励民营部门的所有者和运营商为其控制的基础设施提供最佳的切实可行的安全措施，并向政府提供必要的信息以评估其任务的完成情况。为了充分吸引民营部门，首先要确保民营部门的所有者和运营商均为自愿参加。
- 与州和地方政府以及应急人员紧密配合，对一个强大灵活的基础设施保护方案来说必不可少。所有的关键基础设施保护计划和举措都应当考虑到州和地方政府以及应急人员的需求、行动和责任。

六、组织架构

联邦政府设立 4 个组织（详见附件 A）。

（一）负责部门联络的领导机构

每一个可能会遭受重大网络攻击或者武力攻击的基础设施部门，都会有一个单独的美国政府部门作为其领导机构负责部门联络。每一个领导机构将设立一个助理国务卿级别或者更高级别的部门联络官负责，并与该领域的民营部门代表（部门协调员）在解决涉及关键基础设施保护问题方面开展合作，特别是关于《国家基础设施保护计划》中的推荐部分。该领导机构将同民营部门的相应人员共同研究部署一项针对该部门的“漏洞认知和教育方案”。

（二）负责特殊职能的领导机构

此外，涉及特殊职能的关键基础设施保护则必须主要由联邦政府来完成（主要指国防、外交、情报、执法）。每一项特殊职能都将有一个领导机构负责协调美国政府在该领域的所有活动。每个领导机构将委派一名助理国务卿或者更高级别的高级官员作为“职能部门协调员”负责联邦政府的该项职能。

（三）跨部门的协调

在关键基础设施协调组（CICG）的帮助下和负责安全、基础设施保护及反恐的国家协调员的主持下，“部门联络官”和“职能部门协调员”以及其他相关部门和机构的代表，包括美国国家经济委员会负责协调该总统令的实施。国家协调员将由总统通过负责国家安全事务的总统助理任命并向总统报告，以确保与负责经济事务的总统助理妥善配合。派往 CICG 的机构代表应是高级别的（助理国务卿或者更高级别）。CICG 将在合适的方面得到更大范围政策部门的协助，如安全政策委员会、安全政策论坛和国家安全通信与信息系统安全委员会。

（四）国家基础设施保障委员会

按照领导机构、国家经济委员会和国家协调员的推荐，总统将组建一个专家组，由主要基础设施提供商、州和地方政府官员组成，为国家基础设施保障委员会服务。委员会主席由总统任命。国家协调员将担任委员会执行理事。委员会将定期举行会议，加强政府与民营部门在保护关键基础设施方面的合作关系并酌情向总统报告。联邦政府高级官员将酌情参与委员会会议。

七、保护联邦政府的关键基础设施

联邦政府的各个部、局都有义务保护各自的关键基础设施，特别是基于网络的系统。各部、局的首席信息官（CIO）有义务保障信息安全。各部、局都要设立一名首席基础设施保障官（CIAO），负责该部门关键基础设施所有其他方面的保护。根据各自部门的具体情况，CIO 可兼任 CIAO。这些官员应当建立适合的、有效的授权流程以对政府计算机和物理系统开展漏洞评估。司法部将建立提供相关授权的法律指南。

从总统令发布之日起 180 天内，各部、局应制定其保护自身基础设施的计划，包括但不局限于基于网络的系统。国家协调员有义务协调分析跨部门的各部、局的需求，并调和各部门之间的关系。CICG 必须指定一个专家负责这些计划的审查过程。从总统令发布之日起两年内，这些计划应当实现并且每两年更新一次。为了确保按期完成任务，联邦政府应就如何最好地保护关键基础设施为民营部门提供一个模型。

八、任务

主管委员会应在 180 天内向总统提交一份制定国家基础设施保证计划的日程表，该表应包含下列任务。

（一）漏洞分析

每一个经济部门和政府部门的基础设施都有可能成为将对美国造成重大损失的攻击目标，因此，应进行初始漏洞评估并定期更新。评估还应根据各部门情况确定各部门最不可或缺的基础设施。

（二）补救计划

基于上述漏洞评估，应设定一个补救计划。该计划应确定实施时间、责任和经费。

（三）警报

将立即建立一个基础设施遭受重大攻击的国家级警报中心（见附件 A）。我们尽可能在不久之后，建立一个增强系统来检测和分析这类攻击，并将尽可能引入民营部门参与。

（四）响应

建立一个能在基础设施遭受重大攻击时隔离并减少损失的响应系统。

（五）恢复

对于不同层次、已经成功实施的针对基础设施的攻击，要建立一个系统用于迅速恢复最低要求的运行能力。

（六）教育与宣传

针对政府和民营部门设立安全漏洞的宣传和教育项目，以提高工作人员对安全的重视程度，并培训他们遵守安全标准，特别是网络系统安全。

（七）研究和开发

联邦政府出资的对基础设施保护的研究应与多年计划一致并服从于多年计划，同时要考虑民营部门的研究，并投入足够的资金，以尽快减少漏洞。

（八）情报

情报机构应制定并实施一项计划，加强对国外威胁我国基础设施的情报的收集和分析，应包括但不局限于外国网络战或信息战的威胁信息。

（九）国际合作

应制定计划在保护关键基础设施方面加强同理念相似的盟友、国际组织和跨国公司的合作。

（十）立法和预算要求

在涉及关键基础设施方面，行政部门应有立法权和预算优先权的评估，并在必要时向总统提出改善建议。如有评价建议，都应与预算办公室（OMB）负责人协调。

CICG 应审查并安排附件 B 中的各项任务。

九、实施

除了这份 180 天内提交的报告，国家协调员会同国家经济委员会，将通过负责国家安全事务的总统助理向总统和各部、局的负责人提供一份该总统令的年度实施报告。该报告将包括一份升级版的威胁评估，一份实现国家计划和附加政策要求达到的重大事项的状态报告，以及立法和预算建议。如有评价建议，都应与预算办公室（OMB）负责人协调。此外，在 2000 年达到初步的保障能力之后，国家协调员应进行一次从头开始的审查。

十、附件 A：组织架构

领导机构：美国政府明确的问责制须指定特定的部门和功能。按照职责分配如下。

1. 部门联络的领导机构

商务部：信息和通信。

财政部：银行和金融。

环境保护局（EPA）：供水。

交通部：航空、高速公路（包括汽车和智能运输系统）、大宗货物运输、输送管道、铁路、水路贸易。

司法部/美国联邦调查局（FBI）：应急执法服务。

联邦应急管理局（FEMA）：应急消防服务、政府服务连续性。

卫生及公共服务部（HHS）：公共健康服务，包括预防、监测、实验室服务以及公民健康服务。

能源部：电力、石油和天然气生产和储存。

2. 特殊职能的领导机构

司法部/FBI：执法和国内安全。

中央情报局（CIA）：国外情报。

国务院：国外事务。

国防部：国防。

此外，美国国家科学和技术政策办公室（OSTP）负责通过美国科学技术委员会（NSTC）为政府协调研究、发展议程和项目。虽然商务部是信息和通信事务的领导机构，但国防部仍保留对全国通信系统（NCS）的行政代理责任并为国家安全通信咨询委员会（President's National Security Telecommunications　Advisory Committee）提供支持。

（一）国家协调员

有关国家安全、基础设施保护和反恐的国家协调员应负责协调第 63 号总统令的实施。国家协调员将通过负责国家安全事务的总统助理（国家安全顾问）向总统报告。当主管委员会（Principals Committee）或代理委员会（Deputies Committee）讨论有关基础设施问题时，国家协调员也可作为正式成员出席。尽管国家协调员并不管理某些部门和机构，但他们将确保跨部门协调以推进政策的发展和实施，并将重审有重大外资投入有关基础设施的危机事件。国家协调员将在既定年度预算下，为关键基础设施的机构预算提出建议。国家协调员主持关键基础设施协调组（CICG）的工作，并向首长或次长会议汇报。部门联络官（Sector Liaison Official）和特殊职能协调员（Special Function Coordinator）也应参加 CICG 的会议。部门和机构须各自任命一位 CICG 的高级官员（助理部长级别或以上）定期参加会议。国家安全顾问应在国家安全委员会（NSC）的工作人员中任命一人作为关键基础设施协调组的高级主管。

国家计划协调组（NPC）的工作人员在合法的情况下无偿为机构和部门服务。NPC 将不同部门的计划整合进国家基础设施保证计划，并对美国政府本身依赖的关键基础设施进行协调分析。NPC 也将帮助协调一个国家教育和意识培训项目，以及立法和公共事务。

1998 年国防部应继续对过渡委员会办公室负有行政责任，过渡委员会办公室是形成 NPC 的基础。1999 年年初，NPC 应作为商务部的一个办公室。美国人事管理办公室应为促进 NPC 的运营提供帮助。除非总统令延长，否则 NPC 将在 2001 年年末结束组建。

（二）预警和信息中心

作为国家预警和信息分享系统的一部分，总统授权美国联邦调查局（FBI）将现有机构扩充成一个覆盖全面的国家基础设施保护中心（NIPC）。NIPC 应作为国家关键基础设施威胁评估、预警、脆弱性和执法机构调查和响应的实体。在第 63 号总统令开始实施的半年至一年中，总统可直接指派国家协调员、部门联络官、部门协调员、特殊职能协调员、国家经济委员会（National Economic Council）的代表与关键基础设施的所有者和工作人员合作，以鼓励下文所述民营部门分享和分析系统的建立。

国家基础设施保护中心（NIPC）将包括 FBI、美国特勤局（USSS）、在计算机犯罪和基础设施保护方面有经验的学者，以及国防部、情报部门和领导机构的代表。NIPC 将与联邦政府的其他部门，包括其他的预警和运作中心，以及任一民营部门的分享和分析系统相连。其任务包括为蓄意威胁提供及时预警、综合分析和执法机构的调查与回应。

所有的行政部门和机构应与 NIPC 合作，并在法律认可范围内对 NIPC 提出诸如信息和建议的请求提供帮助。在法律允许的范围内，所有的行政机构应与 NIPC 共享有关网络攻击的威胁和预警信息，以及针对政府和民营部门关键基础设施的攻击信息。NIPC 的职能有预警、分析、计算机搜索、应急协调响应、培训、技术工具的外延、发展和应用。此外 NIPC 将直接与民营部门以及由民营部门所创建的信息共享和分析机构建立联系。

NIPC 联合信息源机构，去除执法信息和情报信息后以适当的格式将其他信息纳入其分析和报告中，提供给相关联邦政府、州和当地机构，关键基础设施的所有者和运营商，以及任一民营部门信息共享和分析实体。在传播来自情报机构有关国家安全等信息之前，NIPC 将在现有流程下与情报机构进行充分的合作。无论是经过筛选的信息还是原始报告，NIPC 将向共享信息的民营部门、分析实体、基础设施的所有者和运营商发布攻击警报或威胁因素增长预警。警报也可能包括有关关键基础设施的所有者和运营商应采取的额外保护步骤的相关指南。除非在极端紧急情况下，否则在发布有关国际恐怖分子、外国或其他恶意国外势力突发攻击的公共预警之前，均应与国家协调员协商。

NIPC 将为收集关键基础设施的威胁信息提供国家性的信息交汇点。此外，NIPC 将提供方法以促进和协调联邦政府对突发事件的响应，减少攻击，弄清威胁并监测重建进度。根据一个国外威胁和攻击的性质和程度，特殊职能机构（司法部、国防部、美国中央情报局）以及总统的最终决定之间须达成协议，无论是国防部还是其他情报机构，NIPC 都将给予其直接的支持。

（三）信息共享和分析中心（ISAC）

国家协调员与部门协调员、部门联络官、国家经济会议一起同关键基础设施的所有者和运营商进行协商，以鼓励民营部门创建信息共享和分析中心。在第 63 号总统令颁布的 180 天内，国家协调员在 CICG 和国家经济会议的帮助下为促进 ISAC 的建立提供政府援助找到可行方法。

该中心可作为一个聚集、分析、适当选取并向工业和 NIPC 传播民营部门信息的机构。ISAC 也可将来自 NIPC 的信息进行汇聚、分析并传播至各个民营部门。关键在于分享有关脆弱性、威胁、入侵和异常的重要信息时并未影响政府和企业之间直接的信息交换。

最终由民营部门所设计的 ISAC 可能仿效诸如美国疾病控制与预防中心此类机构所证明的行之有效的方面，特别是其在民营部门与非联邦部门广泛的接触上。在这样的模式下，ISAC 将有大量的技术性焦点和专业知识，以及非监管和非执法性的任务。该机构将基于各种基础设施建立基础统计和模式，成为各个部门内部和之间的信息交换中心，为民营部门、政府以及 ISAC 所认可的机构提供历史数据库。ISAC 成功的关键在于其及时性、可获得性、协调性、弹性、可用性和可接受性。

十一、附件 B：附加任务

（一）国家协调员应委托研究的课题

- 在信息共享过程中由于民营部门参与而引起的责任问题。
- 着眼于通过提案移除信息共享中已有的法律障碍，包括通过与美国法律学会合作建

立相关模型。

- 文件和信息分类的必要性和这种分类对有效传播的影响，在利用这些方法和信息系统时应安全分享威胁和脆弱性信息，同时避免泄露或泄露给滥用之人而导致的不可挽回的风险。
- 包括安全的传播和信息掌握系统在内的已改善的保护措施不应被泄露，其中含有工业界交易秘密和其他机密商业数据、执法机构信息和证据资料、国家机密安全信息、已披露的有关民营部门基础设施脆弱性的非机密材料以及其他非涉密信息。
- 与国外机构分享对美国基础设施安全有益的信息的意义。
- 已选中的关键基础设施提供商所强制、资助或协助提供的保险，以及那些希望与美国合作的外国关键基础设施提供商所要求的保险的安全标准的潜在益处。

（二）公众传播

为了提升公众对基础设施保护问题的敏感度，须采取以下行动。

（1）在国家协调员的监管下，白宫需要与相关的内阁机构考虑以下议题。

- 会议将汇聚公共和民营部门的国家级领导人一起为增进信息安全提出计划。
- 召集工程、计算机科学、商业和法律的学者重审信息安全教育的现状，并确认现有课程和资源的变化能满足国家在信息安全领域对于专业人士的需求。
- 讨论有关计算机伦理学的问题。

（2）美国国家科学院和美国国家工程院应与工业界相关的联邦政府机构、州和地方官员以及学术带头人展开圆桌会议，以发展提升关键基础设施安全性的国家策略。

（3）情报机构和执法机构应扩大已有项目，并向基础设施所有者、运营商以及政府高级官员进行简要概述。

（4）国家协调员应建立一个包括公共和民营部门高级官员在内的基础设施模拟项目，并向其报告哪些部分可拆分为一个宣传项目；与民营部门协商推出一个连续的国家性宣传项目，以强调提升基础设施安全性的重要性。

（三）联邦政府内部行动

为了使联邦政府提升其基础设施安全性，应立即采取以下行动。

- 美国商务部、总务管理局（GSA）和国防部应协助联邦机构完成与其相关的信息安全保障的最佳实践。
- 国家协调员须对已有的联邦政府、州和地方官员所承担的信息安全保障任务重审进行协调，并对这些机构如何更高效地运转提出建议。
- 所有的联邦政府应对谁有权限进入其计算机系统有明确的指示。
- 情报机构应提升和形式化针对美国关键基础设施的国外网络/信息威胁信息收集和分析的优先级。
- 美国联邦调查局、特工处以及其他机构应大量招募计算机技术相关专业的全职本科生和研究生，以及为地区性计算机犯罪小组招募兼职人员；推进包括网络攻击技术分析和研究在内的专业人才的招募和免于流失。
- 美国交通部应与国防部协商开展基于全球定位系统（GPS）国家交通基础设施脆弱

性的全面评估。该调查应包含发起一项针对基于 GPS 民用系统独立、综合的风险评估，以期基于该评估对现代化国家空域系统（NAS）最终架构做出决定。

- 美国联邦航空管理局应开展并完成一个综合性的国家空域系统安全项目，以保护现代化的 NAS 免受信息安全中断或攻击。
- GSA 应对与基础设施保障相关的大型采购（如新的联邦通信系统 FTS2000）予以确认，研究该项采购是否反映基础设施保护的重要性，必要时应提出建议修改整个采购过程。
- 美国政府管理预算局（OMB）应指导联邦机构根据《政府绩效与结果法》策略规划和绩效测评框架分配基础设施保障任务。
- 负责落实 NSD-42（美国国家安全电信和信息系统安全的国家政策）的美国国家安全局（NSA），应负责美国政府系统进行拦截和开发的测试评估，发布威胁和脆弱性信息，建立标准，进行实验和开发，以及对有问题的安全产品进行评估。

（四）协助民营部门

为协助民营部门达到并保持基础设施安全性要求，应采取以下措施。

- 国家协调员应与国家基础设施保证委员会一起建议并找到方法鼓励民营企业对包括信息和通信系统在内的关键流程进行定期的风险评估。
- 商务部和国防部应共同与民营部门协商将其专业知识提供给关键基础设施的私人所有者和运营商，以发展与安全相关的最佳实践标准。
- 司法部和财政部应发起一项综合性的研究以统计计算机犯罪人员，与他国遏制计算机犯罪方法进行比较，并找到对青少年计算机犯罪进行遏制和解决的方法。

第 13231 号行政令：信息时代的关键基础设施保护

一、政策

（1）信息技术革命已经改变了商业交易、政府运作以及国家防卫的方式。现在，这三项职能依赖于一个关键信息基础设施组成的相互依赖的网络。本命令授权的这一保护项目应包括长期努力以确保关键基础设施信息系统（包括应急准备通信以及支持此类系统的物理资产）的安全。对于电信、能源、金融服务、制造、水、运输、卫生以及紧急服务部门来说，保护这些系统至关重要。

（2）美利坚合众国以政策形式保护关键基础设施的信息系统的运行免受破坏，以便保护人民、经济、必要的人类及政府服务、美国的国家安全，确保不会频繁发生破坏行为，且发生的破坏行为历时最短、可控，并将造成的损害尽量降至最低。该政策的执行应包括涉及企业和非政府机构的自愿合作。

二、范围

为实现这一政策，应成立一个高级行政分支委员会进行协调工作，熟悉信息系统保护相关的联邦工作和项目，包括：

（1）民营行业关键基础设施、州政府和地方政府的关键基础设施的合作和保护，企业和学术机构的支持项目；

（2）联邦机构和部门的关键基础设施的保护工作；

（3）相关的国家安全项目。

三、成立相关机构

基于上述要求，成立了“总统关键基础设施保护委员会”（以下简称“**委员会**”）。

四、保持已有法令的效力

本命令不改变美国政府部门和机构的现有权力或职责。根据《美国法典》第 44 卷第 35 章以及其他可适用法令授权，高级官员对联邦政府信息系统的安全负责。

（一）行政分支信息系统安全

为支持行政分支部门和机构信息系统的安全，美国行政管理预算局（OMB）局长有责任制定内部相关政策、原则、标准和指南，并监督政府的执行情况。当某个行政部门或机构的安全做法出现关键缺陷时，OMB 局长应为总统和适当部门及机构的首脑提供建议。就这一职能，本委员会应协助并支持 OMB 局长，合理认识与部门和机构信息系统安全有关的项目。

（二）国家安全信息系统

为保证各自职责范围内负责运行的信息系统的安全，国防部部长和中情局局长有责任监督、促进、确保政策、原则、标准和指南的实施。国防部部长和中情局局长应咨询总统国家安全事务助理以及相关部门和机构，为保障支持其他的国家安全信息行政分支部门和机构运转的国家安全信息系统的安全，制定政策、原则、标准和指南。

（1）根据此部分制定的政策、原则、标准、指南比根据上一部分制定的政策等文件需要更严格的保护。

（2）当部门或机构的安全做法出现关键缺陷时，总统国家安全事务助理应当向总统和适当部门或机构首脑提出建议。本委员会或其执行或特别委员会之一应当对项目有理性认识，保持国家安全信息系统的安全和持续性。

（3）行政分支部门和机构首脑的额外责任。行政分支部门和机构首脑有责任和义务为包括应急准备通信系统在内的信息系统以及它们控制下的项目提供并维持足够等级的安全。此类部门和机构的首脑应当确保这些项目的开发和融资（在可用的拨款范围内）能充分应对这些任务区域。成本效益安全应当纳入政府信息系统，特别是那些支持国家安全和其他基本政府项目的关键系统。此外，安全应有利于部门和机构的业务运转，而不是不必要的妨碍。

五、委员会责任

与本命令第四部分所述责任一致，本委员会应当提出政策建议，协调项目，保护关键基础设施的信息系统（包括应急准备通信以及支持此类系统的物理资产）。在履行这些责任的活动中，本委员会应当采取以下措施。

（一）扩大合作范围，与民营行业和州政府、地方政府共同开展合作

和有关行政分支部门和机构商议，协调与民营行业的合作与咨询，以及有关关键基础设施的信息系统（包括应急准备通信以及支持此类系统的物理资产）的保护，这些行业包括：拥有、运行、开发及装备信息、电信、运输、能源、水、卫生和金融服务的企业；协调与州政府和地方政府，以及学界和其他社会相关方面的社团和代表进行合作。

（1）须进行此项工作时，本委员会要协助制定自愿标准和最佳做法，其方式与《美国法典》第 15 章第 7 节一致。

（2）咨询潜在的受影响社区，包括法律、审计、金融和保险社区，在法律允许的范围内，决定共同关注的区域。

（3）协调高级联络官与民营行业机构在关键基础设施保护问题上的活动，这些联络官由总检察长、能源部部长、商务部部长、交通部部长、财政部部长、卫生部部长以及联邦紧急事务管理署署长任命。协调活动所涉及范围在这些部门和机构有关职责内。就这些以及其他相关职能，本委员会应与关键基础设施保障办公室（CIAO）以及商务部国家标准与技术研究所、国家基础设施保护中心（NIPC）、国家通信系统（NCS）一起协调工作。

（二）信息共享

为确保系统创建并得到良好管理，在政府网络运营中心、基于自愿由行业建立的信息共

享和分析中心，以及其他相关的运营中心之间，共享威胁警告、分析、恢复信息，应与行业、州政府、地方政府、非政府机构共同展开工作。就此以及其他相关职能，本委员会应当酌情与 NCS、联邦计算机应急响应中心、NIPC 及其他部门和机构协调工作。

（三）事件协调与危机响应

协调项目和政策，以便响应威胁关键基础设施的信息系统安全事件（包括应急准备通信以及支持此类系统的物理资产）。就这一职能，司法部应当酌情通过 NIPC、NCS 的负责人，以及其他部门和机构，与本委员会进行协调工作。

（四）招募、保留、培训行政分支安全专家

咨询行政分支部门和机构，协调项目，以确保负责保护关键基础设施的信息系统（包括应急准备通信以及支持此类系统的物理资产）的政府雇员得到足够的培训和评估。就这一职能，人事管理局应酌情协调本委员会共同工作。

（五）研究与发展

在保护关键基础设施信息系统（包括应急准备通信以及支持此类系统的物理资产）的联邦政府研发项目上，协调科技政策办公室（OSTP）主任，确保在该领域内，政府活动与企业、高校、联邦资助的研究中心以及国家实验室之间的协调工作顺利进行。就这一职能，本委员会应当酌情与国家科学基金会、国防高级研究计划署以及其他部门和机构协调工作。

（六）与国家安全部门的执法协调

推动反网络犯罪项目，协助联邦执法机构从行政分支机构和部门获得必要的合作。支持联邦执法机构调查涉及关键基础设施信息系统（包括应急准备通信以及支持此类系统的物理资产）的非法活动，配合这些机构与其他负责保护国家安全的部门和机构的协调工作。就这一职能，本委员会应当与司法部、NIPC、财政部、特工处，以及其他相关部门和机构做好协调工作。

（七）国际信息基础设施保护

支持美国国务院协调美国政府项目的国际合作，涵盖国际信息基础设施保护问题。

（八）立法

根据行政管理预算局（OMB）通告 A-19 的规定，在关键基础设施信息系统（包括应急准备通信以及支持此类系统的物理资产）保护的立法工作方面，向各部门和机构、OMB 局长、总统法律事务助理提出建议。

（九）配合国土安全部

根据 2001 年 10 月 8 日颁布的第 13228 号行政令，国土安全部有以下职能：保护关键基础设施信息系统（包括应急准备通信），并在信息系统遭受针对性攻击后恢复系统正常工作。本委员会应配合履行上述职能。总统国土安全助理应配合总统国家安全事务助理，负责定义

本委员会在协调努力保护支持信息系统的物理资产方面的责任。

六、成员资格

（1）本委员会成员应从下列行政分支部门、机构以及办公室选取；此外，有关联邦部门和机构可以参与到本委员会适当的下属委员会之中。本委员会应由一名主席和副主席领导，并由总统任命。其他成员应当是下列高级官员或指派者：

- 国务卿；
- 财政部部长；
- 国防部部长；
- 司法部部长；
- 商务部部长；
- 卫生与公共服务部部长；
- 交通部部长；
- 能源部部长；
- 中情局局长；
- 参谋长联席会议主席；
- 联邦应急管理局局长；
- 总务管理局局长；
- 白宫管理与预算办公室主任；
- 科学与技术政策办公室主任；
- 副总统办公厅主任；
- 国家经济委员会主任；
- 总统国家安全事务助理；
- 总统国土安全事务助理；
- 总统办公厅主任；
- 总统可以指派的其他行政分支官员。

本委员会成员及其指派者应为联邦政府的专职或永久性兼职官员或雇员。

（2）此外，下列官员应作为本委员会成员，并组成本委员会的协调委员会：

- 商务部关键基础设施保障办公室主任；
- 国家通信系统负责人；
- 首席信息官（CIO）委员会副主席；
- 国家安全局信息安全保障主任；
- 中央情报局社区管理事务副局长；
- 司法部联邦调查局国家基础设施保护中心主任；
- 美国联邦通信委员会主席可指定一名代表加入本委员会。

七、主席的职能

（1）主席还应同时担任总统的网络空间安全特别顾问。行政分支部门和代理机构应当尽

一切努力，在法律允许的最大范围内，让主席充分、及时了解本委员会职权范围内的所有程序和议题。经与委员会磋商，主席应召集和主持委员会会议，并制定议程；同时，向相关官员提出政策建议和方案，以确保做好国家信息系统重要基础设施的安全保护工作，包括应急准备通信系统以及支持这些系统的实物资产。为了确保全面协调国家安全委员会（NSC）和国土安全局之间的职责划分，主席应同时向总统国家安全事务助理及总统国土安全事务助理报告。主席应与总统经济政策事务助理协调有关民营部门体系和经济影响的问题，并和 OMB 局长就有关预算和本法案第四部分第一条提到的计算机网络预算和安全问题进行协调。

（2）白宫办公室应安排适当规模的工作人员协助本委员会主席。此外，在法律允许的范围内，根据主席要求，经总统办公厅主任批准，行政分支机关各部门和机构的负责人被授权选派或指派内部工作人员到委员会任职。本委员会工作人员的职责范围涉及国家安全信息系统、通信系统和信息化战争，同时受命于总统国家安全事务助理。

八、常务委员会

（1）委员会可视情况设立常务委员会和特别委员会。常务委员会代表不应仅限于在委员会里的这些部门和机构，也可包括其他有关行政分支机关部门和机构的代表。

（2）常设和特设委员会的主席应充分、定期地向委员会报告日常活动，确保各委员会之间工作协调一致。

（3）建立以下常务委员会。

- 民营部门、国家和当地政府外联委员会，由商务部部长指派的人员主持，配合国家经济委员会主席指派人员的工作。
- 行政部门信息系统安全委员会，由 OMB 局长指派的人员主持。该委员会应协助 OMB 在符合《美国法典》第 44 卷第 35 章规定以及其他适用法律的前提下，履行其职责。
- 国家安全系统执行机构。国家安全通信和信息系统安全委员会，须根据国家安全指令第 42 款（NSD-42）建立，由国防部主持，并作为委员会的常务委员会，且重新命名为国家安全系统委员会。
- 应急响应协调委员会，由司法部部长指派的人员和国防部部长指派的人员共同主持。
- 研究和开发委员会，由科技政策办公室（OSTP）主任指派的人员主持。
- 国家安全和应急准备通信委员会。将国家通信系统（NCS）委员会更名为国家安全和应急准备通信委员会。

上述常务委员会已确立的报告职能应遵守 1984 年 4 月 3 日颁布的第 12472 号总统行政令，不应改变其中所载的任何职能或作用。

- 物理安全委员会，由国防部部长指派的人员和司法部部长指派的人员共同主持，协助保障关键基础设施信息系统的物理安全，包括应急准备通信以及支持这种系统的实物资产。常务委员会应协助国土安全局，并应与负责访问记录的物理安全工作组和信息安全政策协调委员会紧密合作，确保工作协调一致。
- 基础设施相关性委员会，由交通运输部部长指派的人员和能源部部长指派的人员共同主持，互相协作以评估个别风险、威胁以及与关键基础设施信息系统相关的漏洞，

包括有效发展模式、仿真以及该领域的其他分析工具和成本高效的技术。

- 国际事务常务委员会，由国务卿指派人员主持，负责帮助国务院协调美国政府的国际合作项目。
- 金融和银行信息基础设施常务委员会，由财政部部长指派人员主持，应当包含来自银行和金融机构的监管部门的代表。
- 其他委员会。其他常务委员会可以由委员会设立。

（4）小组委员会。各常务委员会的主席可以成立必要的小组委员会，并由本委员会主席确定组织成员。

（5）流线型组织。委员会应当制定相应流程，明确自身或下属委员会履行先前政策协调委员会分配的职责的方式方法。委员会应当协同科学与技术政策办公室（OSTP）主任，审查根据第 12472 号行政令设立的联合电信资源委员会的职能，并就其未来角色提出建议。

九、规划与预算

（1）本委员会应当定期提出国家计划，或者为其职权范围内的议题提出计划。委员会还应当协同国土安全办公室（Office of Homeland Security），在审议相关项目的要求和资源后，就委员会监管范围之内的行政部门和机构的预算问题，向 OMB 提出建议。

（2）总统行政办公室下属的行政办公室，在法律允许的范围和拨款的预算内，应当在办公室主任的指示下，向委员会提供诸如人员、资金和管理的支持。仅由第 13228 号行政令设立的、提供给国土安全办公室的资金，可用于上述目的。在法律允许的范围内且必要的情况下，委员会的代表机构也可以向委员会提供行政支持。国家安全局应确保委员会的信息和通信系统得到适当的保护。

（3）根据 1981 年 12 月 4 日颁布的第 12333 号行政令的规定，委员会每年可要求国家科学基金会、能源部、交通部、环境保护局、商务部、国防部以及情报机构，将它们为示范项目和研究向 OMB 提交资金的预算请求列出，以支持委员会的工作。

十、总统顾问小组

委员会主席应当与政府以外的负责给总统出谋划策的高级专家小组紧密合作，尤其是根据 1982 年 9 月 13 日颁布的第 12382 号行政令修订版设立的国家安全电信顾问委员会（NSTAC），以及根据本行政令设立的国家基础设施顾问委员会（NIAC）。上述两个专家小组的主席和副主席也可与委员会会晤，在法律允许的范围内，酌情提出民营部门的观点。

（一）NSTAC

NSTAC 负责向美国总统就对国家安全和应急准备方面至关重要的通信系统的安全性和稳定性提供建议。

（二）NIAC

NIAC 负责向美国总统就支撑其他经济部门（银行与金融、交通、能源、制造）及应急政府服务的关键基础设施信息系统的安全性，提供建议。NIAC 的成员应当由总统任命且不

超过 30 人。NIAC 成员应当从民营部门、学术界、州和地方政府中选出，应当具备与 NIAC 职能相关的专业知识，一般应当从那些业内负责支撑经济领域关键部门（包括银行和金融、交通、能源、通信）及应急政府服务的信息基础设施安全性的行业首席执行官（以及其他组织同等职位的领导人）中选择。NIAC 成员不得为联邦政府行政部门的全职官员或员工。

（1）美国总统应当从 NIAC 成员中指定一名主席和副主席。

（2）本行政令确立的委员会主席将担任 NIAC 的执行主任。

（三）NIAC 的职能

NIAC 将定期召开会议：

（1）加强政府与民营部门在保护关键基础设施信息系统方面的合作，适时就此问题向总统汇报；

（2）提出和制定鼓励民营企业对关键信息和通信系统进行定期风险评估的方法；

（3）监测民营部门的信息分享和分析中心（ISAC）的研发情况，向委员会就如何最大限度地促进这些组织与 ISAC、NIPC 和其他联邦政府机构的进一步合作提供建议；

（4）通过委员会向总统提交报告，应确保根据本行政令的相关条款，与总统经济政策助理进行适当的协商；

（5）向负责关键基础设施的主要机构、部门协调员、NIPC、ISAC 和本委员会提供建议。

（四）NIAC 的行政职能

（1）NIAC 可以举行听证会，进行行为调查，并在适当的时候设立小组委员会。

（2）若 NIAC 主席提出要求，在法律允许的范围内，行政机关各部门的负责人应当向理事会提供与其职能相关的信息和建议。

（3）联邦政府的高级官员在适当的情况下可以参加 NIAC 的会议。

（4）成员在理事会的工作没有补贴。但是，根据个人间接为联邦政府服务工作的法律授权，可以支付成员的差旅费，包括日常必需的出差津贴。

（5）在法律允许的范围和拨款的预算内，商务部应当通过 CIAO 向 NIAC 提供行政服务、工作人员，以及对 NIAC 履行职能可能必要的其他支撑服务和专款。

（五）总则

（1）《联邦顾问委员会法》修订版也适用于 NIAC，根据该法案，除了向国会提交报告外，总统还应当根据商务部依据联邦总务署（Administrator of General Services）所制定的指导方针和程序来履行职能。

（2）理事会应当在本行政令颁布之日的两年后解散，总统在此日期前延长理事会工作时间的情况除外。

（3）撤销 1999 年 7 月 14 日颁布的第 13130 号行政令。

十一、国家通信系统

技术的变革正促使很多的通信系统、数据转播和互联网通信网络融合到一张互连的网络之网中。NCS 和其国家协调中心应当支持使用通信系统、融合化信息、语音网络和新一代应

急准备网络，以及第 12472 号行政令分配的国家安全通信职能。该命令给各部门和机构授予的权力和分配的责任，包括 NCS 主管的角色，维持不变，经本行政令明确修改的除外。

十二、反间谍活动

委员会应当与国家反间谍部门协调行动，以防委员会职权范围内的计划遭受敌对外国情报机构威胁。

十三、分类授权

在此，根据 1995 年颁布的第 12958 号行政令修订版，或者具有相同效力的行政令，授予委员会主席第一时间将信息划分为“绝密信息”的权力。

十四、总则

（1）本行政令不能替代法律规定的任何要求。

（2）本行政令在法律或公平上，不会创造任何实质性或程序性、具备法律效力的，损害美国，美国的部门、机构或其他实体，美国的官员或雇员，或者其他任何人员的权力或利益。

第 13636 号行政令：增强关键基础设施网络安全

一、政策

关键基础设施反复受到网络攻击显示出我国提升网络安全水平的必要性。针对关键基础设施的网络威胁持续增长，是我国目前面临的最严重的国家安全问题之一。面对这些威胁，要保障美国的国家和经济安全，必须要保证关键基础设施的有效运行。我们要通过政策，加强国家关键基础设施的安全和恢复能力，保持一个良好的网络环境，在促进公民安全、国家安全、商业机密、隐私和公民自由的同时鼓励高效、创新和经济繁荣。要达到这些目标，我们要和关键基础设施的业主、运营商达成合作关系，增强网络安全信息共享，共同制定和执行基于风险意识的工作标准。

二、关键基础设施

此法令中所述的关键基础设施是指，对美国有重要意义，一旦失效或者受损会对公民安全、国家经济安全、国家公共卫生或国家安全造成严重影响的相关系统和资产（包括物质形态和非物质形态）。

三、政策协调

为本法令中所描述和归类的职能与项目服务的政策协调、指导、纠纷调解和定期进行的评审，须提交通过 1 号总统政策令（2009 年 2 月 13 日签署的《国家安全委员会组织》）或其后续指令中确立的部际程序讨论或具有相等法律效力的程序。

四、网络安全信息共享

（1）美国政府制定此政策是为了提高与美国民营部门主体共享网络威胁信息的容量、速度和质量，以便这些部门主体能够在面对网络安全威胁时更好地自我保护和防御。此法令签署后 120 天之内，司法部部长、国土安全部部长（以下简称“部长”）以及国家情报总监应行使各自的职权，根据本法令中第十二部分第三条所述要求，发布具体的操作办法，确保及时地向美国公众发布非涉密并明确针对主体的网络安全报告。操作办法应解决保护情报与执法信息源、方法、行动和调查之间的矛盾。

（2）部长、司法部部长应协同国家情报总监建立一套工作程序，用于向目标主体快速传播依本法令第四部分第一条所产生的报告。此工作程序还应包括，出于国家安全信息需要，将涉密报告告知有知情权的关键基础设施经营主体。部长、司法部部长应协同国家情报总监建立上述报告制定、传播和部署的追踪系统。

（3）为协助关键基础设施业主和运营商保护关键基础设施不受未经授权的接入、占用或损害，部长应在遵守《美国法典》第 6 篇第 143 节的基础上与国防部部长合作，在本法令签

署 120 天内，建立覆盖所有关键基础设施部门的强化网络安全服务项目的操作流程。自愿信息共享项目将向有资质的、为关键基础设施提供安全服务的公司和商业服务供应商发布政府官方的机密网络安全威胁和技术信息。

（4）根据 2010 年 8 月 18 日签署的第 13549 号行政令——《面向国家、地方、部落和民营部门实体的机密级国家安全信息项目》，部长作为机密级国家安全信息项目的代理人，应加速关键基础设施业主和运营商的雇佣职员获得安全许可的过程，优先推进本法令第九部分中认证的关键基础设施。

（5）为使网络威胁信息共享在民营部门得到最大化利用，部长应在目前的基础上，增加民营部门的领域专家进入联邦服务项目。这些专家应向关键基础设施业主和运营商提出最有裨益的信息内容、结构和类型建议，降低和减轻网络风险。

五、隐私权和公民自由权利的保护

（1）相关机构应在本法令和上级主管的指导下协调行动，保护隐私和公民自由，并确保将保护隐私和公民自由纳入活动中。每个机构在开展活动时对隐私和公民自由的保护工作，应根据《公平信息实践原则》（FIPP），以及其他隐私与公民自由政策、原则和框架文件来执行。

（2）首席隐私官、国土安全部门（DHS）公民权利与公民自由的主管官员应评估本法令中 DHS 承担职责和项目中会出现的隐私和公民自由的风险，同时应向部长以公开报告的方式，在本法令签署一年内，建议合理的方式来最小化此类风险。本法令涉及的相关资深机构中负责保护隐私和公民自由工作的官员，须主持自身机构的评估工作并在报告中为 DHS 提供评估意见以供参考。此份报告应每年度评审，如有必要可做修改，也可包括机密级的附件。评估意见应包括对《公平信息实践原则》及其他可用的隐私与公民自由政策、原则和框架下所进行活动的评估。报告还应考虑，在开展相关机构活动的过程中，关于如何实现对隐私和公民自由保护的评估和建议内容。

（3）在制作上述报告时，首席隐私官、DHS 公民权利与公民自由的主管官员应与隐私与公民自由监管委员会商讨，并与行政管理预算局（OMB）协调。

（4）根据《美国法典》第 6 篇第 133 节，民营企业依照本法令自愿提交的信息受法律最大程度的保护，不会遭到泄露。

六、协商程序

部长应建立一套协商程序，协调促进关键基础设施网络安全水平的提高。作为协商程序中的一环，部长应参与并思考来自关键基础设施合作咨询委员会，产业协调委员会，关键基础设施业主和运营商，特定行业机构，其他相关行业，独立监管机构，国家、地方、区、部落政府，大学学府和外界专家关于本法令规定问题的建议。

七、建立基础框架降低关键基础设施的网络安全风险

（1）商务部部长应指导国家标准与技术研究所（NIST）主任（以下简称“主任”）牵头建立《降低关键基础设施网络安全风险的框架体系》（以下简称“《网络安全框架》”）。《网络

安全框架》应包括一系列的标准、方法、步骤和程序，以使政策、商业和技术手段结合起来共同解决网络风险问题，还应包括自愿达成的统一标准和尽可能充分的最佳产业实践案例。如果自愿国际标准能提高本法令的目标，《网络安全框架》应与该标准保持一致，还应符合新修订的《国家标准与技术研究所法》（《美国法典》第 15 篇第 271 节）、1995 年的《国家技术转移和推进法》（《公共法》第 104～113 条）和修订后的行政管理预算局（OMB）的第 A-119 号通告的要求。

（2）《网络安全框架》应提出一套优先、灵活、可重复、基于实践、成本低的方案，包括信息安全措施和控制，帮助关键基础设施业主和运营商识别、评估和管理网络风险。《网络安全框架》的重点在于如何确定可用于关键基础设施的多部门安全标准和指导意见，还应确定哪些领域的安全工作有待未来通过和特殊部门、标准研发部门的合作而获得提高。为促进技术创新并考虑到组织机构间的差异，《网络安全框架》还应提供指导，包括技术中立、让关键基础设施部门能从竞争的市场中获利。在这个竞争的市场中，产品和服务应符合可解决网络风险问题的标准、方法、步骤和程序。《网络安全框架》应提供指导，评估主体执行网络安全框架的情况。

（3）《网络安全框架》应通过多项举措确认并减轻本身的影响，协助信息安全措施和控制在商业机密中发挥作用，保护个人隐私和公民自由。

（4）在研究《网络安全框架》的过程中，主任应参与公共评审和评论的流程。部长、国家情报局主任和其他机构的负责人应向《网络安全框架》开发提供网络威胁及脆弱性信息和技术经验。部长还应根据本法令第九部分的要求，提出《网络安全框架》的实施目标。

（5）在本法令签署 240 天之内，主任应发布《网络安全框架》的初稿（“初步框架”）。在本法令签署 1 年内，和部长协商确保初步框架符合本法令第八部分的要求后，主任应发布《网络安全框架》的最终版本（“最终框架”）。

（6）根据法定职责，主任要确保《网络安全框架》和指导通过评审，必要时要更新信息，考虑技术变更、网络风险变化、关键基础设施业主和运营商的实践回馈、本法令第八部分的执行经验和其他相关因素。

八、自愿性关键基础设施网络安全项目

（1）部长在与特定行业机构协调后，应建立自愿性项目（以下简称“项目”）支持关键基础设施业主和运营商、其他相关主体采用《网络安全框架》。

（2）特定行业机构在与部长、其他相关机构商讨后，应协同部门协调委员会评审《网络安全框架》，必要时研究执行意见或补充材料，应对行业风险和改善运营环境。

（3）特定行业机构应每年通过部长向总统汇报关于参与项目的关键基础设施业主和运营商的工作情况（本法令第九部分会注明）。

（4）部长应协调建立一系列鼓励措施，提高各主体的项目参与度。在本法令签署 120 天内，国土安全部部长和财政部部长、商务部部长应通过国土安全和反恐助理、经济事务助理，分别向总统作出推荐报告，包括对这些鼓励措施的好处和有效性的分析，证明这些措施是否合法，或者现行法律和权力是否允许这些措施应用在项目当中。

（5）在本法令签署 120 天之内，国防部部长、总务长官应和部长、联邦并购监管委员会协商，通过国土安全和反恐助理、经济事务助理，向总统作出推荐报告，包括将安全标准并

入合并计划和合约管理的可行性、安全利益和相关优点。报告还应提出具体的步骤，使现有的采购要求与网络安全要求达成和谐与一致。

九、识别处于最大危险的关键基础设施

（1）在本法令签署 150 天之内，国土安全部部长应使用一个基于风险考虑的方法，对一旦发生网络安全事件，就会在地区或者全国范围内对公共卫生安全、经济安全或国家安全产生灾难性影响的关键基础设施进行识别确认。基于此目标，部长应利用本法令第六部分确立的协商程序和特定行业机构经验，还应使用一致、客观的标准识别关键基础设施。本部分所述不包括任何商业信息技术产品或消费信息技术服务。部长应遵照本部分所述，每年评审或者更新已识别的关键基础设施名单，并通过国土安全和反恐助理、经济事务助理将名单提交总统。

（2）特定行业机构主管和其他相关机构应向部长提供必要信息，以遵照本部分要求履行职责。部长应为其他相关方研究信息提交程序，方便各方协助其做好本部分第一条要求的识别工作。

（3）部长应协同特定行业机构，对被识别出的关键基础设施（根据本部分第一条要求）业主和运营商发出秘密通知，告知他们已被识别，并确保被识别出的业主和运营商对此决定做好准备工作。部长还应建立一项程序，便于关键基础设施业主和运营商根据本部分第一条要求提交相关信息和申请复议。

十、框架的采用

（1）负责监管关键基础设施的机构应参与与 DHS、OMB 和国家安全人员的协商过程会议，共同评审初步网络安全框架，并判定目前的网络安全监管要求是否能够应对当前和预期的风险。在做出判定前，这些机构应考虑，根据本法令第九部分，对关键基础设施的识别问题。在初步框架发布 90 天之内，以上机构应通过国土安全和反恐助理向总统提交一份报告，同时通过经济事务助理向 OMB 局长提交报告，陈述机构是否有清晰权限，在网络安全框架上提出要求，合理应对关键基础设施、现已识别的权力机构和其他有需要的权力机构当前和预期的风险。

（2）如果监管要求不够完善，在最终框架发布 90 天内，本部分第一条指出的有关机构应在遵照第 12866 号行政令（1993 年 9 月 30 日签署，《监管计划和评审》）、第 13563 号行政令（2011 年 1 月 18 日签署，《提高监管与监管评审水平》）和第 13609 号行政令（2012 年 5 月 1 日签署，《推进国际监管合作》）的前提下，提出优先的、基于风险意识的、高效和协调一致的行动方案，减轻网络风险。

（3）在最终框架发布两年内，本部分第一条指出的有关机构应在遵照第 13563 号、第 13610 号行政令（2012 年 5 月 10 日签署，《确认与减少监管负担》）的前提下，与关键基础设施的业主和运营商协商，向 OMB 提出报告，指出关键基础设施网络安全要求中存在的任何低效、冲突或过度繁重的条款。报告中要阐述有关机构所做的工作，对采取进一步的行动减轻或清除此类要求做出建议。

（4）部长应协调技术援助部门帮助本部分第一条指出的有关机构做好网络安全框架人员

和项目的开拓工作。

（5）应鼓励负责关键基础设施网络安全监管工作的独立监管机构，参与到部长、有关行业机构和其他可优先采取行动的相关方的协商程序中，各尽其能，共同减轻关键基础设施的网络风险。

十一、定义

（1）“机构”除《美国法典》第 44 篇第 3502 节（5）中定义的独立管理机构外，还包括《美国法典》第 44 篇第 3502 节（1）中描述的美国任何一个权力部门。

（2）“关键基础设施合作咨询委员会”由国土安全部建立(《美国法典》第 6 篇第 451 节)，负责在联邦政府、私有部门以及州政府、地方政府、区政府、部族政府中，就关键基础设施防护活动，进行有效的交互与协调工作。

（3）“公平信息实践原则”是国家战略在网络空间可信身份（NSTIC）附录 A 中提出的八项原则。

（4）“独立管理机构”参见《美国法典》第 44 篇第 3502 节（5）。

（5）“部门协调委员会”是指由关键基础设施业主或运营商的某个特定部门代表组成的一个私有协调委员会。其中，特定部门指由国家基础设施防护计划（NIPP）或者其他后续计划指定的部门。

（6）“特定行业机构”参见 2013 年 2 月 12 日发布的第 21 号总统政策指令《关键基础设施的安全与恢复力》或其他后续指令。

十二、总则

（1）本法令的执行遵守现有法律及拨款条件。本法令并不是提供一个权威机构来管理关键基础设施的安全，并未赋予它法律之外或者超越现存法律界限的权力，也不会更改或限制一个机构在现有法律下的任何权力和责任。

（2）本法令不能使美国行政管理和预算局预算、管理、立法提议的职能有所减弱或产生其他影响。

（3）出于情报、执法依据及运作方法的保护考虑，依据本法令所采取的所有行动应当严格遵守当局管理要求。在支持智能化、强化法律执行效果的特定行动与组织方面，该行动不能取代用于保护完整性和安全性的生效法律。

（4）本法令应当遵守美国国际义务法。

（5）本法令无论在形式或实质上，所采取的法律或道德手段均不悖于美国政党的权力或者利益，生效对象包括美国的部门、机构、组织、官员、雇员、代理人或者任何其他人。

第 21 号总统政策指令：关键基础设施的安全与恢复力

一、主题

为推动各方维护并加强关键基础设施的安全和恢复能力，保证这些设施的顺畅运行，特发布关于关键基础设施的安全与恢复力的总统政策指令（PPD）。

二、介绍

国家关键基础设施为美国社会的正常运转提供必要的服务。有必要维护并加强关键基础设施（包括对树立公众信心以及确保国家安全、繁荣和福利至关重要的资产、网络及体系）的安全和恢复能力，保证这些设施的顺畅运行。

国家关键基础设施复杂多样，涵盖了分布式网络、各式各样的组织结构及运作模式（包括跨国合作）、在实体空间与网络空间领域相互依存的功能系统，以及多层政府、责任及法规的治理结构。关键基础设施的所有者和运营者尤其要设法应对其经营与资产所面对的风险，并采取有效措施使它们更加安全、更具恢复力。

必须确保关键基础设施安全、可承受风险并且能够快速从各类危机中恢复。为实现这一目标，需要整合国家准备系统的各个方面，包括预防、保护、缓和、应对及恢复。

此项指令针对关键基础设施安全与恢复力制定了国家政策。政策的执行需要联邦、州、地方、部落及领地（SLTT）的各级实体，以及关键基础设施公私所有者与运营商共同分担职责。该指令还阐明了联邦政府在关键基础设施方面的相关职能、角色与责任，加强了整体协调与合作。同时，联邦政府有责任加强其自身关键基础设施的安全与恢复力，以确保国家基本职能体系的持续运行。联邦政府也有职责与关键基础设施所有者和运营商有效合作，加强关键基础设施安全与恢复力建设。

三、政策

美国出台政策，加强关键基础设施的安全与恢复力以应对物理威胁和网络威胁。鉴于所有威胁因素都将对国家安全、经济稳定、公众安全与健康的单方面或者多方面造成不利影响，联邦政府应当与关键基础设施的所有者和运营商、SLTT 实体合作，采取积极举措应对风险，加强国家关键基础设施的安全与恢复力。这些举措将力求在关键基础设施上减少漏洞、减轻不良后果、鉴别并消除威胁、快速采取应对与恢复措施。

联邦政府还应与国际社会通力合作，加强国内关键基础设施及国家所依赖的位于境外的关键基础设施的安全与恢复力。

美国针对加强关键基础设施的安全与恢复力所采取的举措是整体性、全盘性的，以此反映基础设施间的相互关联、相互依存。该指令还指出，能源与通信系统尤为重要，它们是所有关键基础设施提供服务的必要条件。

以下三项战略性要务将促进联邦政府加强关键基础设施的安全与恢复力。

（1）改进并明确联邦政府内部职责关系，促进全国共同努力，加强关键基础设施的安全与恢复力。

（2）通过为联邦政府确立基准数据和系统要求进行有效信息交流。

（3）履行整合与分析职能，通报有关关键基础设施的计划与执行决议。

关键基础设施为政府基本事务的日常运作提供支持。联邦政府所有部门与机构的负责人对各自所在单位内部关键基础设施的鉴定、优化、评估、修缮及安全负责。这些基础设施须在《国家连续运行政策》（NCP）计划及执行中体现。

联邦政府各部门与机构应当依据相关法律、总统指令及保护公民隐私、权利与自由的联邦法规来执行该指令。另外，联邦政府各部门与机构应当以符合相关法律条例与政策的方式保护执行指令过程中所涉及的所有信息。

四、角色与职责

此项指令的有效执行须依照国土安全部部长的战略指导，在全国各方共同努力下实现。这不仅需要联邦部门与机构的专业能力或支持能力、与关键基础设施所有者和运营商以及 SLTT 实体组织的强有力合作，还需要特定部门机构（SSA）的专业技术与日常参与。尽管该指令中提到的角色与职责的明确对象为联邦部门与机构，但与关键基础设施所有者和运营商以及 SLTT 实体组织的有效合作对于加强国家关键基础设施的安全和恢复力同样必不可少。

五、国土安全部部长

国土安全部部长应提出战略指导，协调全国各方力量以推进国家关键基础设施的安全和恢复力建设。在履行《国土安全法》（2002 年）（Homeland Security Act of 2002）修订版所指定的职责的过程中，国土安全部部长评估国家维护关键基础设施的能力及所面临的机遇与挑战，分析关键基础设施所面对的威胁、漏洞以及所有风险可能带来的后果，明确与所有关键基础设施公私领域的有效合作所必需的安全与恢复能力，与 SSA 及其他关键基础设施合作者合作制定国家计划与指标，整合、协调在联邦基础设施安全和恢复力方面的跨领域活动，鉴定并分析关键基础设施领域的主要依存关系，报告国家加强关键基础设施安全和恢复力的举措的有效性。

国土安全部部长的其他角色与职责包括：

（1）确定并优先考虑关键基础设施，与 SSA 及其他联邦部门和机构协调合作，考虑关键基础设施所面对的物理威胁与网络威胁、漏洞以及风险后果；

（2）维护全国关键基础设施中心，该中心可提供态势感知能力，包括有关新趋势、紧迫性威胁、可影响关键基础设施事件态势的整合性、可操作性信息；

（3）与 SSA 及其他联邦部门和机构合作，为关键基础设施所有者与运营商提供情况分析、专业知识及其他技术帮助，促进必要的信息交流与情报获取，加强关键基础设施的安全和恢复力；

（4）与 SSA、SLTT 实体组织及关键基础设施所有者和运营商协调合作，对国家关键基

础设施的脆弱点进行综合评估；

（5）依据法定职责，协调联邦政府对影响关键基础设施的重大网络或物理威胁采取应对措施；

（6）支持司法部部长及执法部门依法对针对关键基础设施的威胁和攻击进行调查和起诉；

（7）与 SSA 及其他相关联邦部门和机构合作并利用其专业知识，采用商业卫星、机载系统及其他部门现有能力等手段，对关键基础设施进行地图和影像绘制、分析及归类；

（8）按照法规要求，就国家关键基础设施工作情况提交年度报告。

六、特定部门机构

关键基础设施的每个行业都各具特色，并具有独特的运营模式及风险状况，具备系统专业知识的特定部门机构对行业发展起到推动作用。确认联邦特定部门与机构的法定或监管权威。利用当前对行业的了解与行业间关系，SSA 将在以下几个方面各司其职。

（1）作为全国加强关键基础设施安全和恢复力的重要一环，与国土安全部（DHS）及其他相关联邦部门和机构协调一致，与关键基础设施所有者和运营商合作，适时和独立监管机构以及 SLTT 实体合作，执行此项指示。

（2）为联邦政府提供特定行业的日常发展动态及合作情况。

（3）依照法定职责及其他相关政策、指令或条例的要求，履行事故管理责任。

（4）适时为特定行业提供技术帮助和咨询，支持、促进其发现漏洞，减轻事故危害。

（5）为国土安全部提供年度选定行业关键基础设施的基本信息以支持国土安全部的法定报告需求。

七、联邦政府附加职责

以下部门与机构，必要时与其他联邦部门和机构以及独立监管机构合作，为关键基础设施的安全和恢复力建设履行专业职能或支撑责任。

（1）国务院应在国土安全部、SSA 及其他联邦部门和机构的协同下，推动他国政府和国际组织加强美国境外关键基础设施的安全和恢复力，并促进有关加强关键基础设施安全和恢复力的最佳经验和方法的全面交流。

（2）司法部（DOJ），包括联邦调查局（FBI），应当在关键基础设施领域开展反恐、反间谍及相关执法活动。对于国外情报人员窃密活动、恐怖分子活动，以及其他一切对国家关键基础设施造成威胁的实际攻击或潜在攻击和破坏活动，司法部都应当调查、处理、起诉，或者将危害降至最低。FBI 应当对国内的网络威胁信息进行整理、分析和发布，同时对国家网络调查联合工作组（NCIJTF）的运行负责。NCIJTF 的成员来自国土安全部、美国情报体系（IC）、国防部，必要时还有来自其他机构的成员，是全国跨机构合作的中心，它协调、整合并分享网络威胁调查的相关信息。司法部部长及国土安全部部长应协调合作，完成各自的关键基础设施任务。

（3）内政部应在政府设施行业所对应的特定机构的协作下，确定、开展并协调国家文物遗迹的安全与恢复工作，并在使用、欣赏这些重要资产的同时减少它们面临的风险。

（4）商务部（DOC）应在国土安全部及其他联邦部门和机构的协调配合下，促使私有行业、研究界、学术界以及政府组织提高与基于网络的体系相关的技术和工具的安全，推进与关键基础设施相关的其他工作的开展，以保障工业产品、原料及服务的及时提供，满足国土安全需求。

（5）国家情报总监（DNI）领导下的美国情报体系（IC）应利用相关职权和协调机制，酌情提供关键基础设施威胁的情报评估，在关键基础设施相关的情报和其他敏感或产权信息上进行协调。另外，遵照总统指示，相关法律，保护国家安全体系的信息安全政策、指令、标准及指导条例应受到监督；相应地，其执行也应受到国家安全体系享有职权的机构负责人监督。

（6）总务管理局应与国防部、国土安全部及其他部门和机构适时协商，提供并支持有关关键基础设施的政府层面的合同，并确保在合同中政府享有对关键基础设施的安全及恢复力的审计权力。

（7）核管理委员会（NRC）应从以下方面对其授权商进行监督：用于研究、试验、训练的商用核反应堆及非能源核反应堆；医疗、工业及实验设施制造核燃料所使用的核材料；核材料及核废物的运输、储藏和分配。核管理委员会应尽可能与国土安全部、司法部、能源部、环境保护署以及其他联邦部门和机构适时合作，加强关键基础设施的安全及恢复力。

（8）联邦通信委员会应与国土安全部、国务部、其他联邦部门和机构、SSA 适时合作，在法律允许范围内，在以下方面行使其职权，运用其专业知识：确定并发展通信基础设施；确定通信行业漏洞并与业界及其他利益相关方合作，解决漏洞问题；与包括通信行业、相关国外政府及国际组织在内的利益相关方合作，加强通信行业关键基础设施的安全及恢复力，促进关键通信基础设施的安全及恢复力最佳实践的开发与使用。

（9）联邦部门和机构应及时为国土安全部部长及国家关键基础设施中心提供信息，以便进行关键基础设施的跨行业分析以及提供态势感知能力报告。

八、三项战略任务

（1）改善并理清联邦政府内部职能关系以促进全国共同努力，加强关键基础设施的安全及恢复力。

加强关键基础设施的安全及恢复力的全国有效行动须以一个确认角色与职能的国家性计划为指导，该计划依据 SSA、其他在关键基础设施中起重要作用的联邦部门和机构、SLTT 实体组织以及关键基础设施所有者和运营商的专业技能、经验、能力及职责制定。

在过去的十年中，我们实施了新项目，采取了新举措以解决特定基础设施的问题，优先发展领域也随之转移和扩大。因此，我们应理清并改善联邦政府在关键基础设施的安全和恢复力方面的职能，以促进反映情况发展的基准能力建设，规定相关联邦政府项目的职能，促进联邦政府、关键基础设施的所有者和运营商以及 SLTT 实体组织间的合作与信息交流。

作为职能关系改善结构的一部分，国土安全部将设立两个国家关键基础设施中心：一个为物理基础设施中心，另外一个为网络基础设施中心。它们将以整体运作的方式，作为服务中心，为关键基础设施的合作者们获取态势感知以及整合性的可操作信息，以保护物理及网络关键基础设施。正如关键基础设施的实体因素和网络因素不可避免地相互关联一样，它们在漏洞方面也密不可分。因此，两个国家关键基础设施中心应共同履行整合和分析职能（具

体情况参见第三项战略任务）。

国家关键基础设施中心的成功运行，包括其整合和分析职能的履行，有赖于 SSA、其他联邦部门和机构、关键基础设施的所有者和运营商、SLTT 实体组织为其提供及时、高质量的信息与情报。

这两个国家中心不应妨碍联邦部门及机构的负责人履行其在国家防卫、犯罪打击、反间谍、反恐以及调查活动方面的职责。

（2）为联邦政府确定基准数据和系统要求，确保有效信息交流。

一个安全、顺畅运转及可恢复的关键基础设施体系要求在各级政府与关键基础设施的所有者和运营商之间实现包括情报在内的信息的有效交流。应当促进有关关键基础设施的威胁、漏洞以及事故中有助于增强态势感知能力的信息的交流。我们的目的是通过明确对数据、信息格式、信息的可获得性以及系统的兼容性方面的要求，保证信息有效交流，做好备用系统及备选措施准备以防主系统遭到破坏。

在考虑到公民隐私与公民自由的前提下，政府内部以及政府与民营行业之间可以而且必须实现更大范围的信息分享。联邦部门和机构应确保所有现有隐私原则、政策及程序在符合相关法律及政策的情况下执行，还应让机构高级官员管理和监督信息分享。

（3）履行整合与分析职能，通知有关关键基础设施的计划与执行决议。

第三项战略任务建立在前两项战略任务基础之上，须承担关键基础设施整合与分析职能，包括对事故、威胁和即将出现的风险的操作性和战略性分析。此项职能应由第一项战略任务中提及的两个国家中心共同完成，包括核对、评估并整合漏洞信息、威胁流所造成的后果分析以及风险信息，以促进以下工作的开展。

- 促进关键基础设施的资产开发及风险处理。
- 预测相关性与串联影响。
- 在事故前、事故中及事故后提出关键基础设施安全与恢复力措施。
- 提供关键基础设施事故处理及恢复手段。

此项战略任务职能不同于情报体系或者国家反恐中心的分析职能，且不涉及情报搜集工作。情报体系、国防部、司法部、国土安全部以及其他掌握相关情报、信息的联邦部门和机构，应为国家中心提供与国家关键基础设施相关的、及时的适当信息，以支持整合与分析职能的执行。信息和情报供给来源还有包括 SLTT 及非政府分析组织在内的其他关键基础设施的合作者。

最后，此项整合和分析职能应支持国土安全部保持并分享对关键基础设施的近实时态势感知能力，包括有关紧迫性威胁、重要趋势方面的可行性信息以及对可影响关键基础设施的事故的警惕意识。

九、创新、研究与开发

国土安全部部长应在科技政策办公室（OSTP）、SSA、商务部及其他联邦部门和机构的协调配合下，为联邦或联邦资助的研发（R&D）活动提供与之匹配的投入。研发活动的目的是加强国家关键基础设施的安全和恢复力，包括：

（1）促进安全和恢复力设计、关键基础设施建设以及更多相应网络安全技术开发等研发活动；

（2）加强决定某一事故或威胁对关键基础设施的潜在影响以及对其他行业的串联影响的建模能力；

（3）采取积极举措，刺激网络安全投资，采纳有利于增强全灾害安全与恢复力的关键基础设施设计特点；

（4）开展工作以支持国土安全部部长的战略指导。

十、指令的执行

国土安全部部长应采取以下措施执行该指令。

（1）关键基础设施安全与恢复力职能关系。自指令颁布日起 120 日内，国土安全部部长应就国土安全部内部及联邦政府中的关键基础设施安全和恢复力的职能关系做出描述。描述包括两个国家关键基础设施中心的角色与职责，以及对其分析整合职能的讨论。职能关系一旦确立，应作为关键基础设施所有者和运营商以及 SLTT 实体组织的路线图，以此来掌舵联邦政府的职能方向，为加强关键基础设施安全与恢复力、应对实体威胁和网络威胁确定职责基本点。就此，国土安全部部长应与 SSA 及其他相关联邦部门和机构协调努力。国土安全部部长应通过总统的国土安全与反恐事务助理，将职能关系描述提交给总统。

（2）对现行政府与民间合作模式的评估。自指令颁布日起 150 日内，在 SSA、其他联邦部门和机构、SLTT 实体组织以及关键基础设施所有者和运营商的配合下，国土安全部部长应对现行政府与民间的合作模式进行分析，并提出提高物理空间和网络空间领域合作效率的方案。评估应考虑对合作和信息交流简化流程，减少重复作业。另外，在为联邦政府提供一个集中、严格、行之有效的合作方法以实现与关键基础设施所有者和运营商、SLTT 实体组织合作的同时，分析还应考虑如何使运作模式灵活适用，以满足个别行业的特殊需求。经国家安全委员会系统组织指示所设立的程序批准，评估中关于加强合作关系的建议才能实施。

（3）为联邦政府确定基准数据和系统要求以实现有效的信息交流。自指令颁布日起 180 日内，在 SSA 及其他联邦部门和机构的协调合作下，国土安全部部长应召集组织一个专家团队，明确基准数据和系统的要求，以使有关关键基础设施的安全及恢复力的信息和情报实现有效交流。团队专家将包括来自掌握日常关键基础设施安全及恢复力重要信息的实体组织的代表、建立并管理用于信息交流的信息技术体系的专家，以及确保信息交流安全的责任人。分析中应包括关键基础设施合作者之间的兼容性，对联邦、SLTT 及民营行业的数据及信息要求的确定，数据的可使用、可获得及格式，交流各种类型信息的能力，所使用系统的安全，以及对公民隐私和公民自由的适当保护。分析应最终制定出对数据共享和系统兼容性的基准要求，实现数据信息的及时交流，以确保关键基础设施安全、更具恢复力。国土安全部部长应通过总统的国土安全与反恐事务助理，将分析材料提交给总统。

（4）培养关键基础设施的态势感知能力。自指令颁布日起 240 日内，国土安全部部长应展示出对威胁流、各种灾害信息及漏洞的近实时性态势感知能力，提供关键基础设施的状况及潜在的串联影响方面的信息，支持决策确立，在事故中传播关键必要信息以拯救或维持生命、减轻破坏或减少关键基础设施能力的再度降级。在关键基础设施的实体领域和网络领域都应具备此项能力，并进行事故所需的信息的整合。

（5）《国家基础设施保护计划》的更新。自指令颁布日起 240 日内，国土安全部部长应通过总统的国土安全和反恐助理向总统提交《国家基础设施保护计划》的后续事宜安排，明

确此指令的执行、《国土安全法案》（2002 年修订版）第二章要求，以及与第 8 号总统政策指令（PPD8）所要求的《国家准备目标和系统》一致。计划应包括用于加强关键基础设施安全及恢复力的风险处理框架、开发关键基础设施的方法、用于同步联邦政府内部交流与行动的协议，以及用于衡量国家处理和降低关键基础设施风险的能力的指标和分析程序。更新计划还应反映国土安全部内部及联邦政府中所确定的职能关系和政府与民间的合作模式的更新。最后，计划还应考虑行业对能源和通信系统的依赖关系，确定事故前预警措施、缓解措施或系统遭破坏时的备用方案。国土安全部部长应与 SSA、其他相关联邦部门和机构、SLTT 实体组织以及关键基础设施所有者和运营商协调合作，开展此项工作。

（6）《国家关键基础设施安全及恢复力研发计划》。自指令颁布日起两年内，在科技政策办公室、SSA、商务部以及其他联邦部门和机构的协调合作下，国土安全部部长应通过总统的国土安全及反恐事务助理向总统提交《国家关键基础设施安全与恢复力研发计划》。计划中应包括关于发展中的威胁趋势、年度指标以及其他确定开发和引导研发要求及投资的相关信息。计划自首次提交起，应每四年发布一次，必要时进行过渡式更新。

为执行此项指令所进行的政策协调、争议解决以及周期性回顾应符合第 1 号总统政策令（PPD1）的要求，包括如何管理利用由国家安全人员协调配合的跨部门政策委员会。

该指令的内容不会改变、取代或者阻碍包括独立监管机构在内的联邦部门和机构在符合相关法律条款及其他总统指令（包括但不限于关于关键基础设施的指示）的情况下履行其职能和责任。

该指令撤销了 2003 年 12 月 17 日颁布的第 7 号国土安全总统指令《关键基础设施的识别、优先级和防护》（HSPD7）。依据 HSPD7 制定的计划在被明确取消或替代之前仍具有效力。

（一）指定的关键基础设施行业及特定部门机构

此指令明确了 16 个关键基础设施行业，指定了相关的联邦 SSA。在一些情况下还指定了联合 SSA，在联合 SSA 中，多个部门共同承担 SSA 的角色与职能。国土安全部部长应做出周期性评估，以决定是否有必要和是否批准对关键基础设施行业进行改变。在进行某一关键基础设施行业或其所对应的指定 SSA 变更前，国土安全部部长应与总统的国土安全和反恐事务助理协商。这些关键基础设施行业及其所对应的 SSA 如下。

化工业：
SSA：国土安全部
商业设施：
SSA：国土安全部
通信行业：
SSA：国土安全部
关键制造业：
SSA：国土安全部
水利系统：
SSA：国土安全部
国防工业基础：

SSA：国防部
应急服务：
SSA：国土安全部
能源业：
SSA：能源部
金融服务：
SSA：财政部
粮农业：
Co-SSA：美国农业部和美国卫生及公共服务部
政府设施：
Co-SSA：国土安全部和联邦总务署
医疗和公共卫生：
SSA：美国卫生及公共服务部
信息技术产业：
SSA：国土安全部
核反应堆、原料及废物：
SSA：国土安全部
交通系统：
Co-SSA：国土安全部和交通部
供水及污水系统：
SSA：环境保护署

（二）定义

词条“全灾害因素”指自然的或人为的威胁或事故，须采取措施以保护生命、财产、环境及公共健康或安全，减少对政府、社会及经济活动的破坏。它包括自然灾害、网络事故、行业事故、流行疾病、恐怖主义行为、破坏活动，以及针对关键基础设施的犯罪破坏行为。

词条“合作”指协调努力以完成共同目标。

词条“协调”和“配合”指达成共识的决策过程，在此过程中，指定的部门或机构有责任与相关部门和机构协调努力以达成共识，采取一致行动。

词条“关键基础设施”参见《美国爱国者法案》（2001 年）[42 U.S.C．5195c（e）]，指对美国至关重要的实体或网络系统及资产，其功能障碍和损害都将对国家安全、经济安全、国民健康或安全的单个方面或多个方面产生削弱影响。

词条“联邦部门和机构”除 44 U.S.C.3502（5）规定的独立监管机构外，还包括 44 U.S.C.3502（1）中规定的美国任何一个权力机构。

词条“国家重要职能”指在灾难性突发事件中领导并维持国家状况的必要政府职能。

词条“基本任务职能”指为了支持突发事件前、事件中及事件后国家重要职能的完成而必须履行的政府职能。

词条“安全国家系统”参见 2002 年《联邦信息处理法案》[44 U.S.C．3542（b）]。

词条“恢复力”指具备应对和适应条件变化、能经受破坏并从中快速恢复的能力，包括

承受并从故意攻击、事故或不可抗力威胁或事故中恢复的能力。

词条“特定部门机构”（SSA）指此指令中所明确的负责下列工作的联邦部门或机构：提供系统知识和专业技能，在风险环境中引导、促进或支持安全和恢复力项目以及所对应的关键基础设施行业的相关活动。

词条“保护”和“安全”指以实际手段或防御性网络措施降低遭受入侵、攻击的风险，减轻自然或人为灾害对关键基础设施的影响。

行政命令：促进民营部门网络安全信息共享

一、政策

美国公共健康与安全、国家安全、经济安全领域都面临着网络威胁。为应对这些威胁，民营企业、非营利组织、行政部门、机构和其他单位必须做到共享网络安全风险和事件的相关信息，并通过合作尽可能地快速应对网络威胁。

共享网络安全风险和事件相关信息的组织机构在美国网络安全中起到不可估量的作用。这则命令旨在鼓励组建这些机构组织，以建立可以持续改进这些机构的能力和作用的机制，允许组织机构更好地与联邦政府在自愿的基础上展开合作。

此类信息共享必须在确保信息安全的基础上，保护个人隐私和公民的自由权，保守商业秘密，同时令政府可以监测、调查、预防和应对针对美国公共健康和安全、国家安全、经济安全领域的网络威胁。

本命令基于 2013 年 2 月 12 日发布的第 13636 号行政令《增强关键基础设施网络安全》和第 21 号总统政策令《关键基础设施的安全与恢复力》。

此处所提的职能和计划将按照 2009 年 2 月 13 日发布的第 1 号总统政策令（《组建国家安全委员会》）中所提及的“跨机构”执行，包括所需的政策协调、指导、解决争议和正在进行的周期性审查，或任何后续命令。

二、信息共享和分析机构

（1）美国国土安全部部长将积极鼓励成立和发展信息共享和分析机构（ISAO）。

（2）信息共享和分析机构可以建立在部门、分部门、地区或其他相关机构的基础上，包括应对特定新出现的威胁或漏洞。信息共享和分析机构的成员可以来自公共或民营部门，或者政府与民间合作的机构。信息共享和分析机构既可以是营利性质，也可以是非营利性质。

（3）根据 2002 年《国土安全法》第 226（b）条成立的美国国家网络安全和通信集成中心（NCCIC）将与信息共享和分析机构，在网络安全风险和事件信息共享、应对未来安全风险和事件、加强信息安全系统等方面，开展持续、协作、兼收并蓄的合作，这也与《国土安全法》的第 212 条和第 226（b）条一致。

（4）在促进信息共享和分析机构组建方面，秘书处将与其他负责开展网络安全工作的联邦机构协商。这些联邦机构包括特定机构、拥有自由裁量权的独立管理机构和执法机构。

三、信息共享和分析机构的标准组织

（1）在与负责执行网络安全和相关行动的其他联邦机构磋商后，秘书处将通过开放和竞争的过程与非政府组织达成协议，成为信息共享和分析机构的标准组织。该标准组织将确定一组通用的自愿性标准或指南，以在此命令下成立和运行信息共享和分析机构。标准将推动

信息共享和分析机构之间形成有力的涉及网络安全风险和事件的信息共享机制，以创建更深层次和更广泛的全国信息共享网络，并培育和发展信息共享的自动机制。标准将提出在这一命令下，信息共享和分析机构需要具备和展示的基本能力。这些标准将指导信息共享和分析机构的运作和成员选择，包括但不仅限于合同协议、业务流程、操作规程、技术手段和隐私保护，例如最小化等。

（2）这些标准组织必须展示出在应对网络威胁和事件信息的大量组织机构中协作的能力。其中包括各信息共享和分析机构、协会和为客户提供支持而信息共享的民营企业。

（3）在本部分第一条中提到的协议，将要求标准组织为上述标准发展召集公开的公众评议和讨论，征集现有的共享网络威胁和事件信息的机构、关键基础设施的所有者和经营者、相关机构、其他公共和民营部门的利益相关方的观点。

（4）秘书处将支持这些标准的发展，并在落实本部分要求的同时，与美国行政管理和预算局、国家标准与技术研究所、司法部、国家档案和记录管理局的信息安全监督办公室、国家情报主任办公室、特定机构和其他相关联邦机构协商。所有的标准都要与自愿性质的国际标准相符，这些国际标准将推进此命令的目标。同时，标准要符合 1995 年颁布的《国家技术转移促进法》和行政管理与预算局发布的经过修订的第 A-119 号通告的要求。

四、关键基础设施保护项目

（1）依照 2002 年的《关键基础设施信息保护法》中的第 213 条和第 214（h）条，将指定 NCCIC 承担一项关键基础设施保护计划，并赋予其与信息共享和分析机构签订自愿协议的权利，以促进关键基础设施安全方面涉及网络安全的防护。

（2）其他与此命令目标相一致的联邦机构也可以在这些协议下参与相关行动。这些联邦机构负责网络安全防护及相关行动，应对针对公共健康和安全、国家安全、经济安全的威胁。

（3）秘书处将决定信息共享和分析机构及其成员是否有资格获取与自愿协议有关的任何必要的帮助或人员安全许可。这依据 2010 年 8 月 18 日签署的第 13549 号行政令《面向国家、地方、部落和民营部门实体的机密级国家安全信息项目》和 1993 年 1 月 6 日签署的第 12829 号行政令《国家产业安全项目》。

五、隐私和公民自由保障

（1）各机构须与其负责隐私和公民自由权的高级机构官员协调行动，以保障在这些行动中，隐私和公民自由权可以得到适当的保护。这些保护措施基于《公平信息实践原则》和其他一些适用于各机构行为、与隐私和自由权相关的政策、原则和框架。

（2）根据总统颁布的第 13636 号行政命令，负责隐私和公民自由权的高级机构官员在行动中将会评估其机构的行动，并将评估报告提交给国土安全部首席隐私官，以及国土安全部的公民权利与公民自由办公室。

六、国家产业安全项目

经过修订的第 12829 号行政命令，现进一步修订如下。

（1）修订第二段，在“修订后的 1947 年《国家安全法》”后增加“2004 年《情报改革

及恐怖主义预防法》”的内容。

（2）第 101（b）条修订如下：“国家产业安全计划将依照 2009 年 12 月 29 日发布的第 13526 号总统行政命令，或任何前任或继任命令，以及修订后的 1954 年《原子能法》（《美国法典》第 42 卷第 2011 条）为涉密信息提供保护”。

（3）第 102（b）条修订如下：将第一节替换为“在与国家安全顾问磋商后，根据 2009 年 12 月 29 日签署的第 13526 号总统行政命令，信息安全监督办公室主任将负责实施和监督全国产业安全计划”。

（4）第 102（c）条修订如下：“本命令中的任何条款都不得解释为可以取代修订后的 1954 年《原子能法》赋予能源部部长或核能管理委员会的权力，或者《2004 年情报改革和防范恐怖主义法》、修订后的 1947 年《国家安全法》或 1981 年 12 月 8 日签署的第 12333 号总统行政命令赋予国家情报局局长（或任何情报机构部门）的权力，或者第 13549 号总统行政命令（《针对州、地区、部落和民营实体的国家安全涉密信息计划》）赋予国土安全部秘书处作为涉密国家安全信息计划的执行机构的权力”。

（5）第 201（a）条修订如下：“美国国防部部长在与所有相关机构协商，并得到美国能源部部长、核管理委员会主任、国家情报局局长和国土安全部部长的同意后，将发布并持续修订《国家产业安全计划操作手册》。美国能源部部长、核管理委员会主任将规定和发布该《操作手册》中属于 1954 年《原子能法》（《美国法典》第 42 卷第 2011 条）的修订过的部分。国家情报局局长将规定和发布该《操作手册》中属于情报资源和方式的部分，包括敏感隔离信息。秘书处将规定和发布该《操作手册》中属于指定的关键基础设施保护计划中的共享的部分信息”。

（6）第 201（f）条全部删除。

（7）第 201（e）条改成第 201（f）条，并将“1982 年 4 月 2 日第 12356 号总统行政命令”修改为“2009 年 12 月 29 日第 13526 号总统行政命令，或任何继任命令”。

（8）第 201（d）条改成第 201（e）条，并将“国家情报局局长与国土安全部部长”修改为“与中央情报局局长”。

（9）在第 102（c）条后插入新的第 102（d）条，内容为“《手册》也将规定在关键基础设施保护计划下，规定必要的安排，以保证涉密信息的安全共享。国土安全部部长将决定授权给哪些个人和组织共享涉密信息”。

（10）第 202（b）条修改为“国家情报局局长保留访问情报资源和手段的权力，包括‘敏感隔离情报’。国家情报局局长可以检查和监督能访问涉密信息的承包商、被许可方、授权的计划和设施；或者与国防部部长签署书面协议，作为其执行机构；或者与中央情报局局长签署书面协议，全权或部分代表中央情报局局长来检查和监督这些计划或设施”。

（11）第 202（d）条改成第 202（e）条。

（12）在第 202 条中，在（c）之后加入全新的（d），内容为“国土安全部部长可以决定在特定的关键基础设施保护计划中，访问涉密国家安全信息的承包商、被许可方、受让人和其雇员的资格；也可以决定这一计划中，达成协议的各方的资格。国土安全部部长可以检查和监督能访问涉密信息的承包商、被许可方、授权的计划和设施；或者与国防部部长签署书面协议，作为其执行机构；或者与中央情报局局长签署书面协议，全权或部分代表国土安全部部长来检查和监督这些计划或设施”。

七、定义

（1）“关键基础设施信息”的定义基于 2002 年《关键基础设施信息保护法》的第 212（3）条。

（2）“关键基础设施保护项目”的定义基于 2002 年《关键基础设施信息保护法》的第 212（4）条。

（3）“网络安全风险”的定义基于 2002 年《国土安全法》的第 226（a）（1）条（由 2014 年的《国家网络安全保护法》修订）。

（4）“公平信息实践原则”为《网络空间可信身份标示国家战略》（NSTIC）中附录 A 所阐述的八条原则。

（5）“事件”的定义基于 2002 年《国土安全法》的第 226（a）（2）条（由 2014 年的《国家网络安全保护法》修订）。

（6）“信息共享和分析机构”的定义基于 2002 年《关键基础设施信息保护法》的第 212（5）条。

（7）“特定机构”的定义基于第 21 号总统政策令或任何继任政策令。

八、总则

（1）本命令的解释不得损害或影响：

- 法律或行政命令赋予机构或其负责人的权力；
- 行政管理与预算局局长涉及预算、行政或立法建议的职能。

（2）本命令执行时应与适用的法律相符，并在经费运行的范围内。本命令的解释不得改变或限制现有法律赋予机构的任何权利和责任，这其中包括与民营部门一起应对犯罪行为和威胁国家安全的行动。本命令的解释不得赋予机构大于现有法律所赋予的管理基础设施安全的权利。

（3）依照本命令开展的行动需要符合保护情报及执法资源和方法的要求和权利。

（4）本命令并不打算或者并不会产生任何实质性或程序性的权力和利益，在法律或实体上被任何人执行，以反对美国政府、各部门和机构，或者政府机构官员、雇员，或代理人，或其他任何人。